Proposition infrastructure



Partie réseau

Une image contenant texte

Description générée automatiquement

Table des matières

[Introduction 3](#_Toc107149644)

[LAN 4](#_Toc107149645)

[1. VLAN 4](#_Toc107149646)

[2. WIFI 6](#_Toc107149647)

[3. Firewalls 8](#_Toc107149648)

[4. Cœur de réseau 12](#_Toc107149649)

[5. Switch de distribution 14](#_Toc107149650)

[6. Switch d’accès 16](#_Toc107149651)

[7. Liaison VPN 17](#_Toc107149652)

[WAN 21](#_Toc107149653)

[1. Fournisseur d’accès à internet 21](#_Toc107149654)

[Recettage 23](#_Toc107149655)

[Site belge 24](#_Toc107149656)

[LAN 24](#_Toc107149657)

[WAN 25](#_Toc107149658)

[Recettage 25](#_Toc107149659)

[Couts totaux prévisionnel 26](#_Toc107149660)

# Introduction

Pour rappel la société MALO profite de son déménagement dans de nouveaux locaux pour remplacer entièrement ses équipements informatiques et les applications qu’elle utilise.

Cette partie constitue l’une des quatre parties de notre proposition faite à la société MALO concernant la restructuration de leur infrastructure.

Nous étudierons ici notre proposition sur l’infrastructure réseau de la société.

Après une analyse complète de l’ensemble des documents fournies par le client (document de question réponse, plans des locaux, consignes, et les différentes demandes) nous avons pris en compte l’ensemble des besoins exprimés par le client que nous pouvons résumer en quatre différents points :

* La pérennité :
  + Proposition d’une infrastructure stable, réaliste et fonctionnelle garantissant un PCA & PRA
* La sécurité
  + Implémentation de la sécurité la plus optimale au sein du réseau
* La cohérence
  + Infrastructure réaliste, correspondant à la taille de la société et au confort des salariés de celle-ci
* L’évolutivité
  + Prise en compte de la forte croissance de la société MALO

# LAN

## VLAN

Le VLAN regroupe, de façon logique et indépendante, un ensemble d’équipements informatiques. Cela évite d'avoir des équipements réseaux différents dans une entreprise lorsque nous voulons que deux départements ou fonctionnalités ne soient pas sur le même réseau ou vu l'un de l'autre.

Nous pouvons noter plusieurs avantages au sein de notre infrastructure grâce aux VLANs comme ;

* Le VLAN réduit la taille des domaines de diffusion.
* Effectuer un regroupement logique des périphériques par fonction plutôt que par emplacement.
* Segmenter facilement votre réseau.
* Renforcer la sécurité du réseau.
* Réduction des coûts
* Augmentation des performances

Nous avons décidé dans notre proposition d’établir une segmentation par types d’équipement au sein de l’entreprise MALO.

1. VLANs segmentés par type d’équipements :

VLAN 10 : Réseau (Switches, borne wifi, firewall = 172.10.210.0/24)

VLAN 20 : Imprimantes (172.10.220.0/24)

VLAN 30 : User (172.10.230/24)

VLAN 40 : Wifi Guest (172.10.240.0/24)

VLAN 50 : Smartphones (172.10.250.0/24)

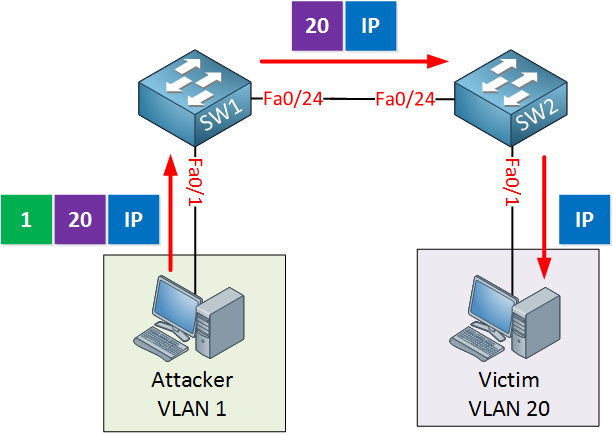
VLAN 60 : Device Corp (172.10.251.0/24

1. Sécurité des VLAN

Concernant la sécurité des VLANs que nous prenons très au sérieux, nous avons pris plusieurs initiatives dans un soucis de cohérence avec la demande du client.

Tout d’abord nous créerons un VLAN 99 qui deviendra le VLAN natif.

Celui-ci prendra en charge les trames untagged et permettra une augmentation de la sécurité contre le « VLAN HOPPING » car le VLAN par défaut n’aura pas d’interface active



Le VLAN Hopping (saut de VLAN) est un exploit en sécurité informatique. Le principe est qu'un hôte attaquant sur un VLAN accède au trafic d'autres VLAN auxquels il ne devrait pas avoir accès

Cette attaque consiste à encapsuler deux champs VLAN dans les trames envoyés. Pour exploiter cette technique, il est nécessaire d'être connecté à un port compatible 802.1Q.

Voici le déroulé de cette attaque :

On envoie d'une trame avec deux champs VLAN encapsulés (le premier correspond au VLAN auquel on a accès et le second celui que l'on souhaite atteindre)

La trame est transmise sans la première balise car il s'agit du VLAN natif d'une interface de jonction (mode trunk)

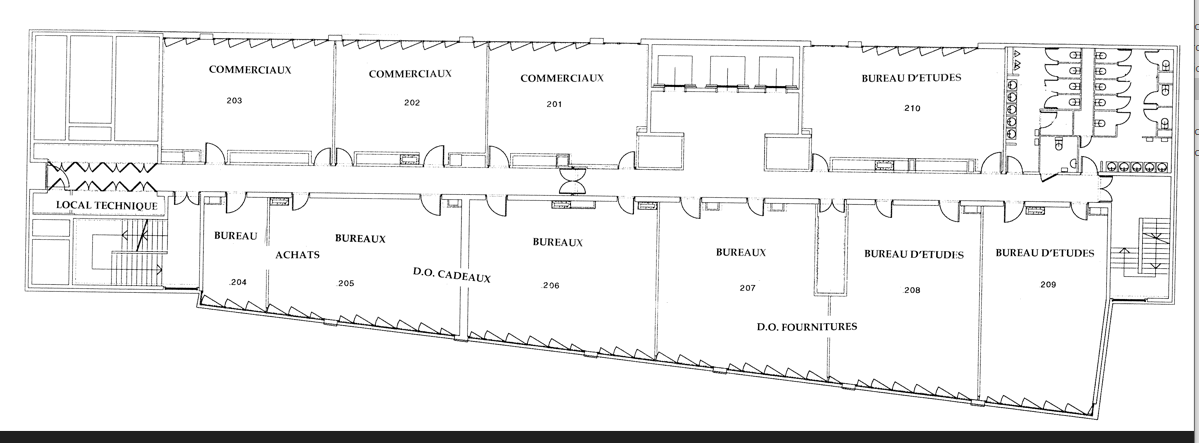
La deuxième balise est alors visible par le deuxième switch que la trame rencontre

Cette deuxième balise VLAN indique que la trame est destinée à un hôte cible sur un deuxième switch

La trame est ensuite envoyée à l'hôte cible comme si elle provenait du VLAN cible, contournant efficacement les mécanismes de réseau qui isolent logiquement les VLAN les uns des autres

## WIFI

Concernant la partie WiFI, nous avons réalisé une étude de couverture à l’aide des plans des locaux fournie par le client



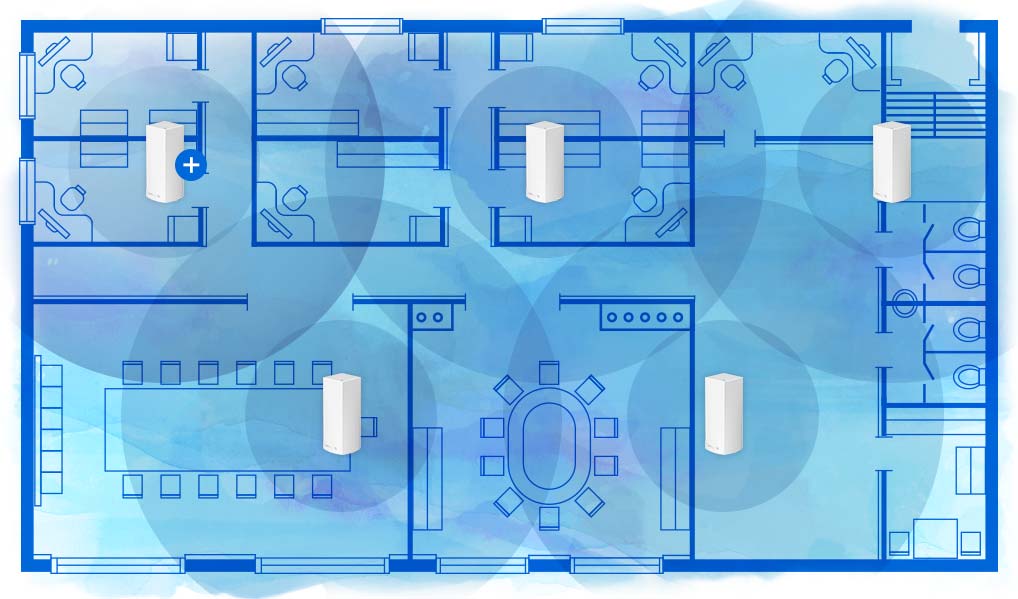
Nous avons déterminé à la suite de cette étude de couverture le besoin de quatre bornes wifi soit un total de 12 bornes wifi pour le siège de la société MALO.

Le plus cohérent concernant les besoins d’évolutivité et de confort des salariés et de proposer une configuration en Wifi-Mesh1

1 Le Wifi Mesh est constitué d’un ensemble de bornes Wifi dont chacune relaie les flux de données. L’ensemble du maillage ainsi créé s’adapte dynamiquement aux volumes de données en répartissant la charge intelligemment pour garantir une stabilité et un débit maximal en toutes circonstances.

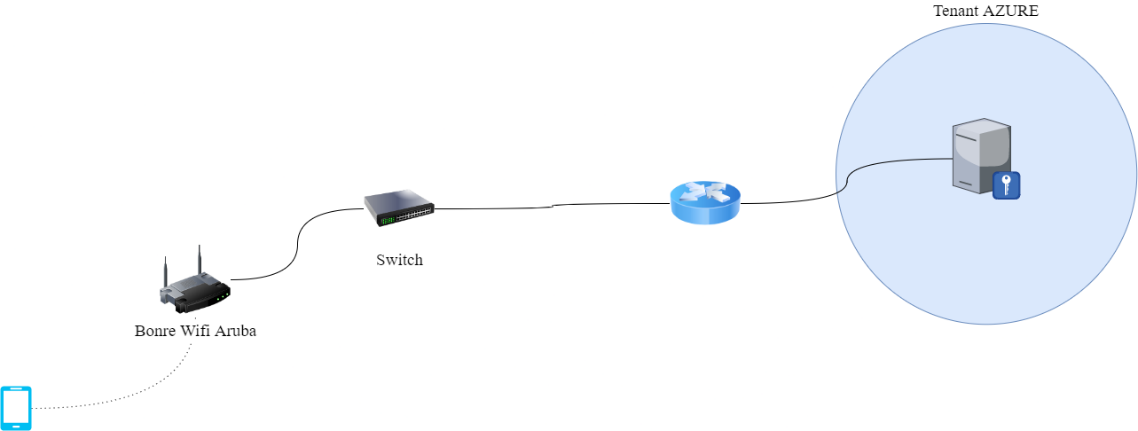
Chaque borne du maillage diffuse 100 % de la puissance reçue de la box et possède le même nom de réseau, pas de confusion possible. À la différence du répéteur, il n’a pas spécialement besoin d’être placé à un endroit spécifique pour répéter le signal correctement. Autre avantage, les appareils se connectent au réseau maillé à la volée de façon automatique et vers le point d’accès le plus puissant sans déconnexion

Pour résumé plus simplement plusieurs bornes forment un seul et même réseau Wi-FI



A la demande du client nous prévoyons la création de trois SSID (Service set identifier)

* Wifi Guest ;
* Wifi Smartphone ;
* Wifi Device Corp ; Authentification RADIUS avec Azure Active Directory (voir partie AD)
  + RADIUS est un protocole conçu pour authentifier les utilisateurs distants d'un serveur avec accès par modem. Dans notre cas nous utiliserons notre service Active Directory sur Azure (Voir partie Azure) pour authentifier les salariés de l’entreprise.



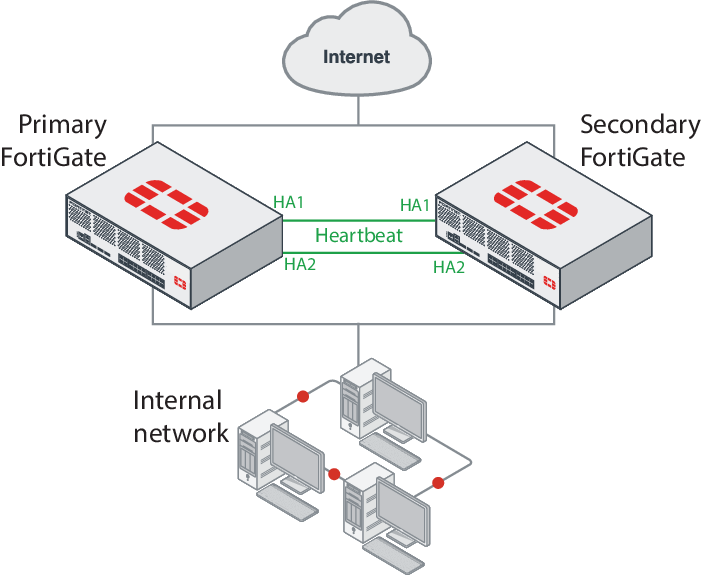
## Firewalls

Le pare-feu protège la totalité du trafic réseau et a la capacité d'identifier et de bloquer le trafic indésirable. Dans notre proposition celui-ci fera également office de routeur.

1. Cluster

Plusieurs options HA sont prises en charge par FortiGate : FortiGate Clustering Protocol (FGCP), FortiGate Session Life Support Protocol (FGSP), Virtual Router Redundancy Protocol (VRRP) et mise à l'échelle automatique dans les environnements cloud.

FGCP est la solution HA la plus couramment utilisée. Il permet à deux FortiGates ou plus du même type et modèle d'être mis dans un cluster en mode Actif-Passif (AP) ou Actif-Actif (AA). Le mode AP offre une redondance en ayant un ou plusieurs FortiGates en veille à chaud au cas où l'appareil principal connaîtrait une panne détectable. En cas de panne, le trafic bascule rapidement vers un périphérique secondaire, évitant ainsi tout temps d'arrêt important. Le mode AA permet d'équilibrer le trafic entre les unités du cluster à des fins d'analyse et effectue également un basculement. Pour FortiGates à la périphérie du réseau, au moins un cluster de deux unités est recommandé.



Après étude précise des besoins nous pensons que la configuration des deux firewall Fortigate en mode actif-actif est la meilleure solution à envisager.

Voici pourquoi ;

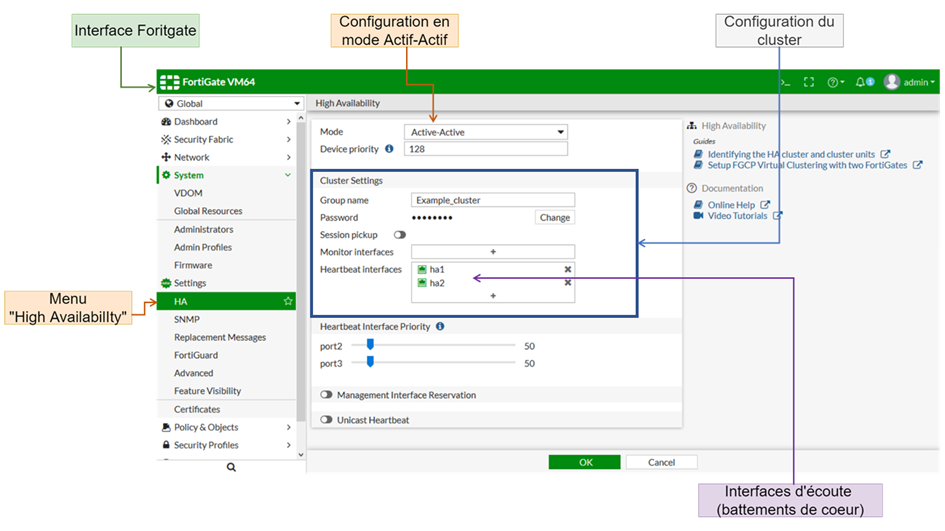
Un cluster actif/actif est une architecture de résilience des données dans laquelle les charges de travail du client sont distribuées sur au moins deux nœuds dans un cluster, afin de préserver la sécurité et la disponibilité de vos données en cas de panne inattendue d’un composant.

Les avantages d’un cluster actifs/actifs ;

* Équilibrage de charge (High Availability)
  + Les flux sont envoyés à charges égales sur le firewall Fortigate 1 et 2
* Redondance
  + Si un firewall venait à tomber en panne l’ensemble du flux serait assurer par le second

Fonctionnement :

Création d’un cluster virtuel (Mac & IP virtuel) et répartition de la charge avec le protocole FGCP (FortiGate Clustering Protocol)



La différence avec un cluster actifs/passifs ;

Dans une configuration actifs/passifs les flux sont redirigés vers le même firewall (firewall principal qui a la priorité la plus élevé dans la configuration) qui gère toute la charge de travail, pendant que le second firewall reste en veille (en passivité) et ne s’active qu’en cas de panne.

1. Switch virtuel

Création d’un switch virtuel à partir des interfaces physiques des deux firewalls pour éviter les boucles (Equivalent protocole Virtual Switching System (VSS) ou Virtual System Framework (VSF))



Avantage du VSS ;

• Taux de convergence entre 100 et 200 ms en cas de panne

• Remplace les protocoles FHRP, HSRP, BRRP, GLBP

• Une seule adresse IP de passerelle par VLAN au lieu de 3 (IP active + IP Passive + IP Virtuel)

1. Matériel proposé

Concernant les deux pare feux, nous avons décidé de privilégier deux FortiGate 400D pour une valeur unitaire d’environ 9 000 euros.



Nous avons entendu les demandes du client sur la sécurité, la pérennité et la qualité de l’infrastructure exigé c’est pourquoi nous avons choisi ce modèle qui est cohérent avec les envies et perspectives d’évolution de la société MALO

## Cœur de réseau

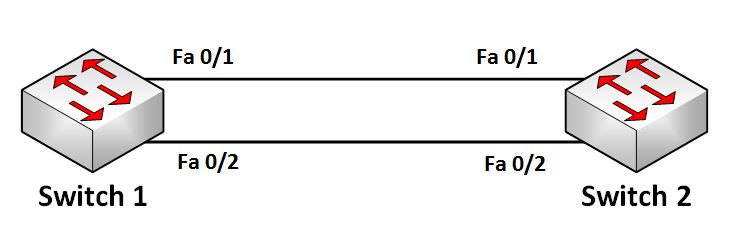
Le cœur de réseau désigne les installations de communication hautement fonctionnelles qui interconnectent les nœuds primaires. Le cœur de réseau fournit des routes pour échanger des informations entre les différents sous-réseaux.

Le switch de cœur est celui qui gère tous les switchs. Les switchs de cœur sont ultra performants pour avoir la puissance nécessaire de gérer une grande quantité de switch.

Dans le cœur de réseau :

L'agrégation de liens (IEEE 802.3ad ou Link Aggregation Control Protocol est un protocole de niveau 2 du modèle OSI) nous permet de lier deux ou plusieurs interfaces physiques pour former un lien agrégé (combiné). Ce nouveau lien a la bande passante de tous les liens combinés. Si une liaison du groupe tombe en panne, le trafic est automatiquement transféré vers les interfaces restantes.

Création d’une agrégation de liens (Etherchannel & LACP pour HP) entre les deux switch cœur de réseau



Les avantages d’une agrégation de lien :

* Meilleure disponibilité
* Répartition de la charge sur les interfaces physiques
* Amélioration de la bande passante

## Switch de distribution

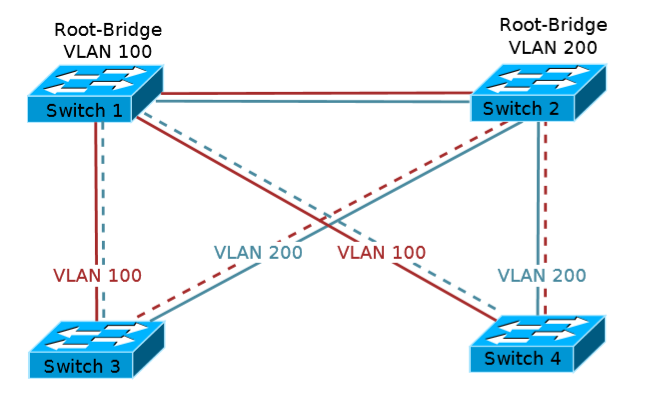
Le switch de distribution permet de gérer les switchs de plusieurs étages, il distribue les connexions et le flux de données de la même façon que le switch utilisateurs mais pour les switchs uniquement.

Concernant cette couche de distribution nous avons souhaité maximiser la bande passante dans notre réseau, et maximiser la haute disponibilité et la redondance nous permettant de garantir un PCA malgré une panne de l’un de nos équipements.

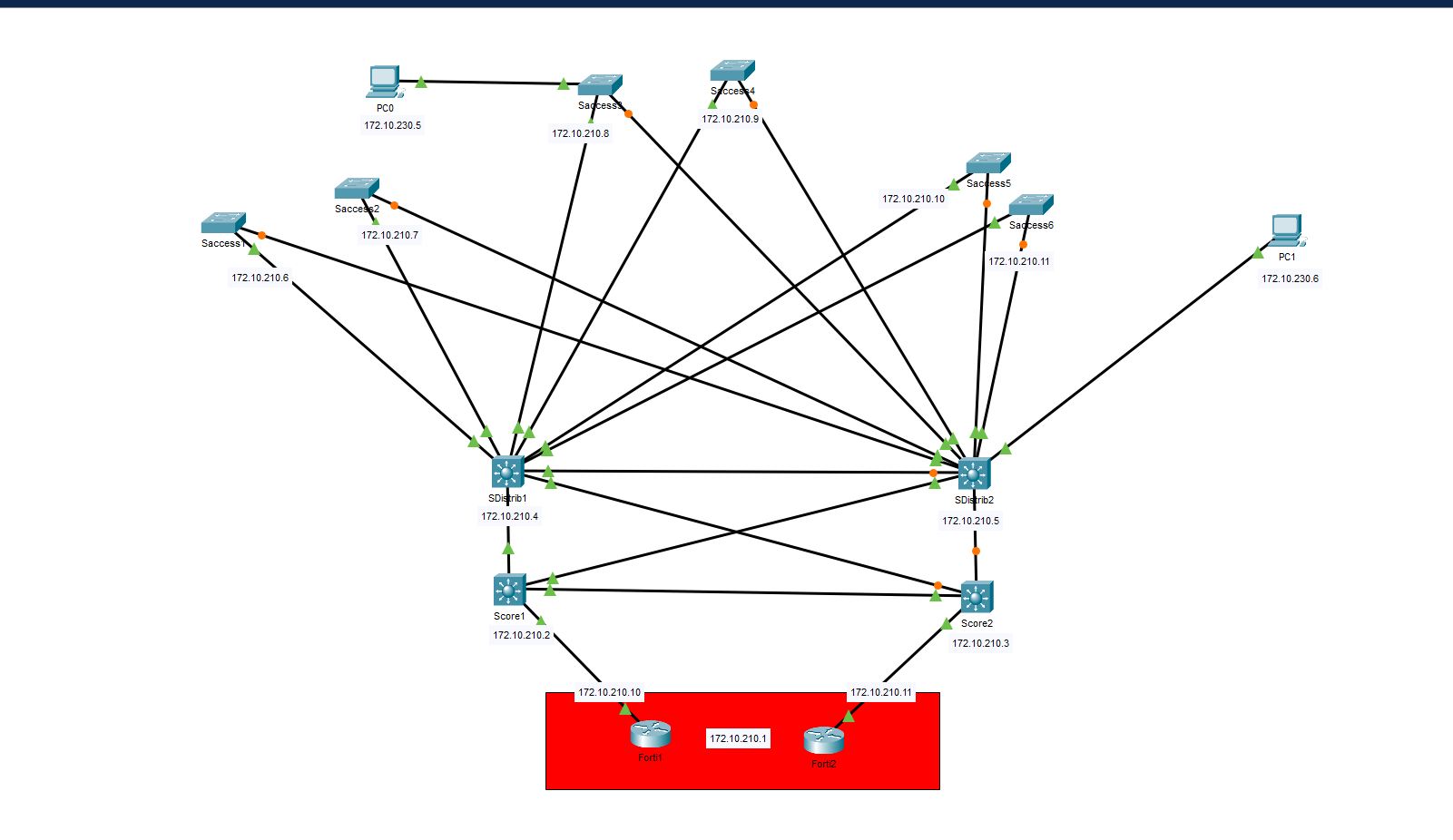
C’est pourquoi nous avons acté sur l’intégration du protocole PVST+ (Per-VLAN Spanning Tree).

Le protocole PVST+ permet à chaque VLAN d’avoir un spanning tree indépendant (et donc éviter les boucles)

Comme ce schéma peut l’illustrer, les interfaces pouvant présenter des boucles de réseau sont temporairement down afin d’éviter les boucles



Plus précisément dans notre infrastructure, voici à quoi cela ressemblera ;



Voici le schéma présenté au client le 8/06/2022 indiquant les interfaces down et up pour éviter les boucles au sein du réseau. Que vous pouvez voir, toutes les interfaces pouvant présenter des boucles réseau sont temporaire « shutter » par le PVST+.

Cette maquette a été testé et validé par le client lors de notre démonstration

## Switch d’accès

Le switch au plus près de l’utilisateur et de l’entreprise. C’est celui qui gère la distribution des connexions d’un étage.

Après analyse des locaux et bureaux nous avons établi un besoin de 2 switch par étage soit un total de 8 switch d’accès

Le modèle privilégié est HPE ARUBA 6100 48G Classe 4

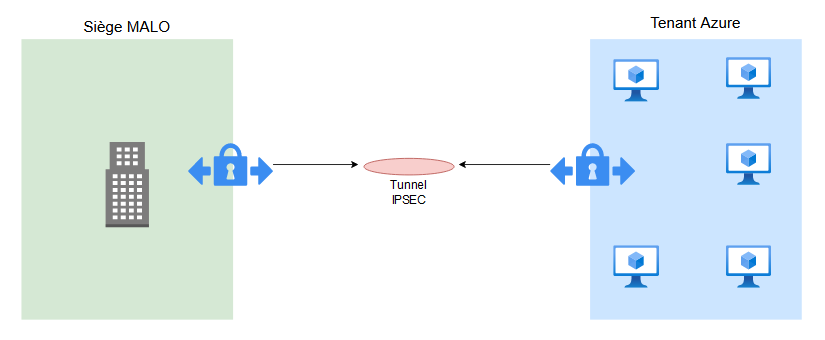
La valeur unitaire de ce switch est 2400 euros, soit un total de 19 200 € pour les 8 switch d’accès

Nous avons choisi ce modèle pour rester dans une cohérence de la marque HP qui sont nos cœurs de réseau et nos switch de distribution. Tous ces modèles présentent donc des combativités de protocoles grâce au même système d’exploitation qui est distribués sur les équipements réseau préalablement choisi par nos soins

## Liaison VPN

Afin de créer une infrastructure stable et cohérente, nous avons besoin d’établir une liaison VPN afin de joindre nos machines virtuelles qui sont dans le cloud de Microsoft, Azure.

Voici une illustration ;

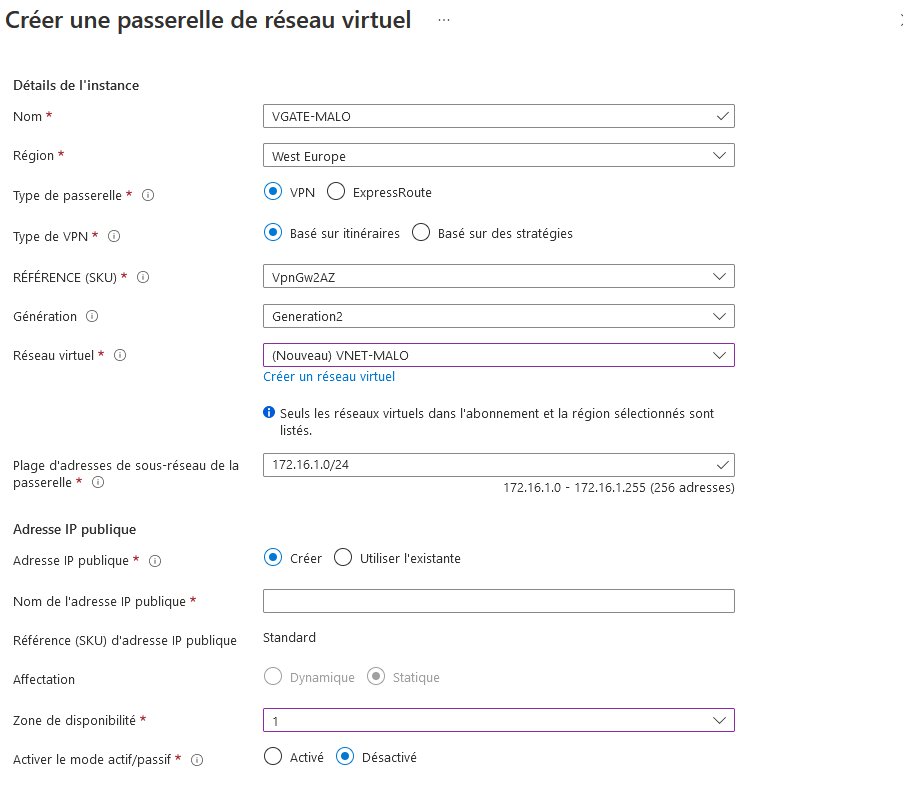


1. Création d’un VirtualNetwork

Depuis Azure une passerelle de réseau virtuel devra être créer afin de créer ce tunnel entre le site physique de la société MALO et les ressources qui sont dans le cloud

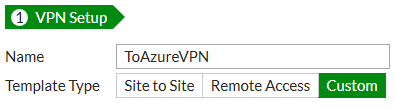
Une image contenant texte

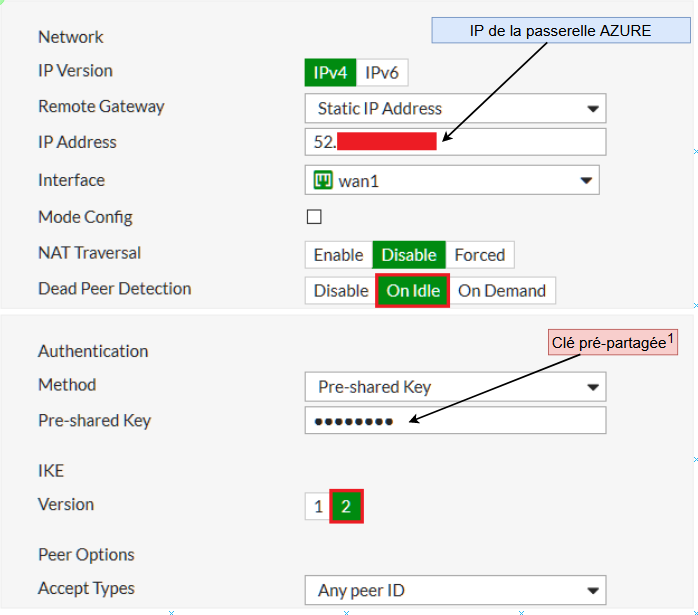
Description générée automatiquement



1. Configuration du tunnel FortiGate

Maintenant depuis nos firewalls physiques nous allons renseigner la passerelle précédemment créer sur Azure afin de lier notre infrastructure physique à Azure

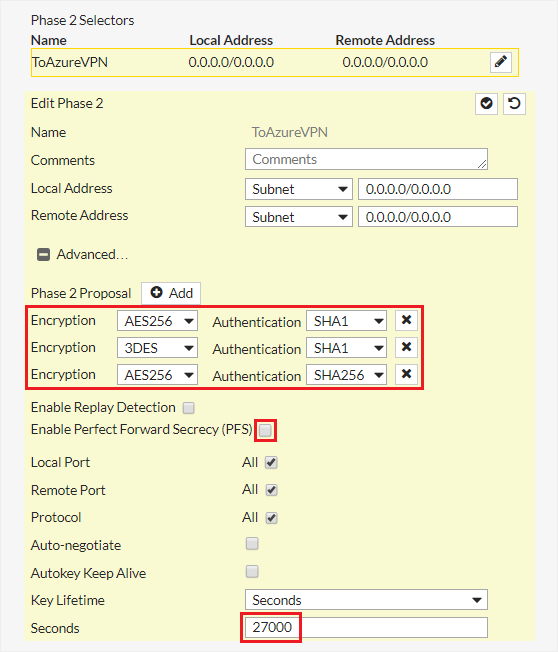




1En cryptographie, une clé pré-partagée est un secret partagé qui était auparavant partagé entre les deux parties en utilisant un canal sécurisé avant de devoir être utilisé

La clé peut être trouvé avec la commande powershell suivante ;

Get-AzureVNetGatewayKey -VNetName “VN-MALO”



1. Création de la route

Une image contenant texte

Description générée automatiquement

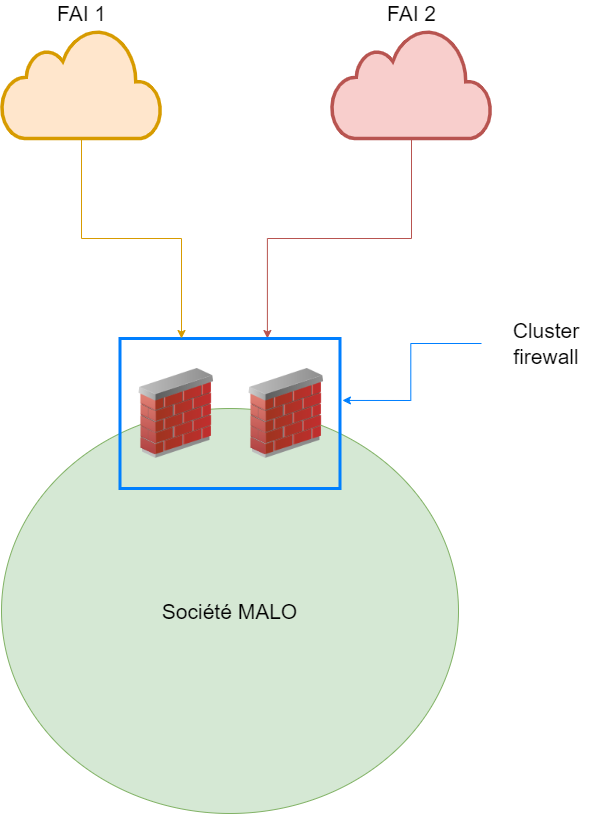
# WAN

## Fournisseur d’accès à internet

Concernant le fournisseur d’accès à internet nous privilégions également une connexion internet redondante.

Une connexion internet redondante ou une connexion internet de secours, est un lien vers internet qui s’active lorsque votre connexion internet est en panne ; assurant ainsi une continuité de service. Aussi, cette connexion internet peut aussi fonctionner en parallèle de la première.

Voici un schéma qui présente synthétiquement une infrastructure avec deux fournisseurs d’accès à internet permettant une continuité d’activité en cas de dysfonctionnement qui pourrait survenir ;



On note différents avantages liés à la redondance de FAI qui sont ;

• Réduction des risques de défaillance du réseau : Le réseau est beaucoup plus susceptible de rester opérationnel avec une redondance de réseau.

• Optimisation du temps et de l'argent : les dommages causés au réseau peuvent coûter du temps, de l'argent et des ressources humaines à l’organisation.

• Augmenter la disponibilité du réseau : la disponibilité du réseau fait référence à la durée de fonctionnement du réseau de l’entreprise. Plus la disponibilité du réseau est élevée, plus les clients et les employés peuvent accéder facilement, rapidement et de manière fiable au réseau de l’entreprise.

• Amélioration de la sécurité de l'entreprise : la redondance du réseau aide à protéger l’entreprise contre les dommages physiques causés au réseau, tels qu'une catastrophe naturelle ou un vol mais également mieux protéger l’organisation contre les menaces de cybersécurité

FAI principal :

Fibre dédié (FTTO), garantie de rétablissement GTR1 débits symétriques 7Gbit/s chez Bouygues Telecom

FAI secondaire :

Fibre FTTH chez Orange

1 Garantie de temps de rétablissement

## Recettage

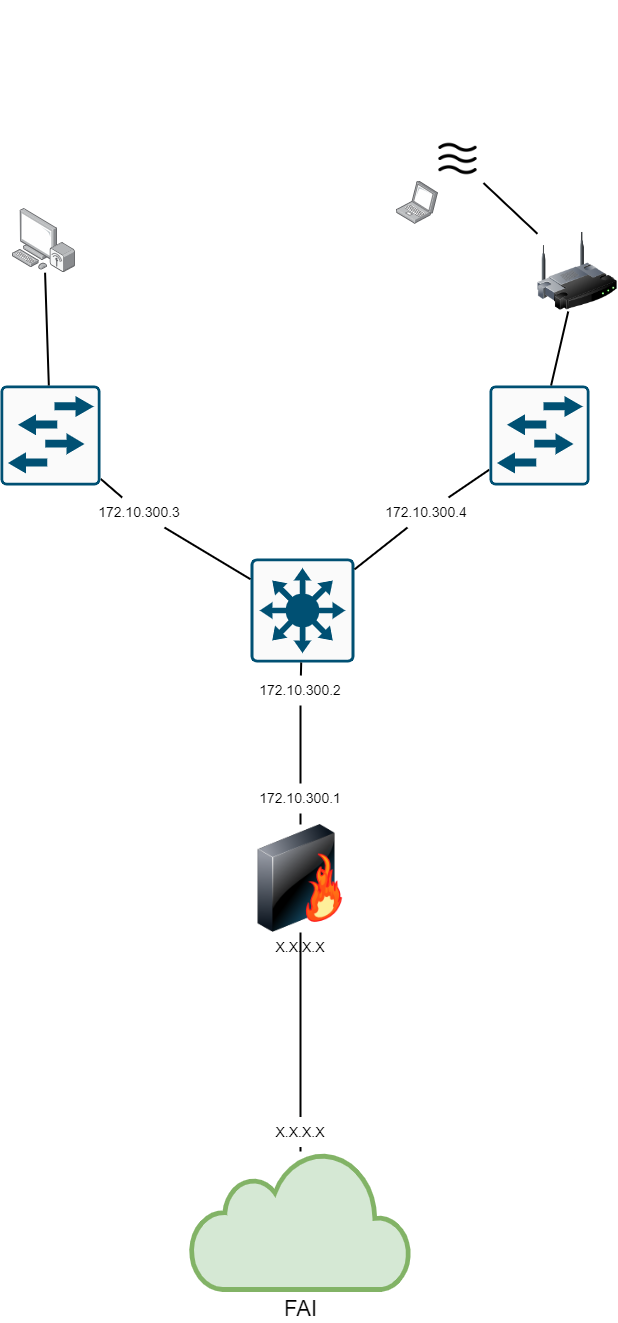
Après avoir étudier l’ensemble des équipements qui seront implémenter dans cette infrastructure, voici maintenant les couts prévisionnels en termes d’équipement pour le site de Paris

|  |  |  |
| --- | --- | --- |
| Modèle | Quantité | Prix du lot |
| Fortigate 400D | 2 | 18 000 € |
| HP JG219B | 2 | 5 821 |
| HPE ARUBA 6100 48G Classe 4 | 8 | 19 200 |
| Bornes wifi Aruba AP505RW | 12 | 5 448 |
| Total |  | 48 469 |

# Site belge

## LAN

Le site de Belgique de la société MALO demande beaucoup moins d’infrastructure en raison d’un nombre de salariés moindre.

D’après les informations que nous avons voici l’infrastructure que nous proposons ;

* + 1 Firewall (Modèle : FortiGate 400D)
  + 1 Switch cœur de réseau (Modèle : HP JG219B)
  + 2 Switch d’accès (Modèle : HPE ARUBA 6100 48G Classe 4)
  + 3 Bornes Wifi (Modèle : Aruba AP505RW)

## WAN



Concernant la connexion internet du site en Belgique nous avons opté sur un connexion internet fibre fournie par l’opérateur Proximus

Le débit garantie se situe entre 500 Mbps à 1 Gbps ce qui sera suffisant en vue du peux d’utilisateur ce le site de Bruxelles

Le tarif mensuel s’élève à 120€

## Recettage

Le cout total de l’infrastructure de la Belgique est représenté dans ce tableau.

Nous retrouvons l’ensemble des équipements définie dans la partie LAN

|  |  |  |
| --- | --- | --- |
| Modèle | Quantité | Prix du lot |
| Fortigate 400D | 1 | 9 000 € |
| HP JG219B | 1 | 2 941 |
| HPE ARUBA 6100 48G Classe 4 | 2 | 4 800 € |
| Bornes wifi Aruba AP505RW | 2 | 850 € |
| Total |  | 17 591 |

Nous avons donc un cout prévisionnel de 17 591€ d’équipement

# Couts totaux prévisionnel

|  |  |
| --- | --- |
| Modèle | Coûts |
| Site Paris | 48469 |
| Site Belgique | 17591 |
| Total | 66 060 |