REFONTE DE L'INFRASTRUCTURE RESEAU

AssurMer

29 JUIN 2021

Cantin LIOTTARD

Sommaire

Présentation de l'étude de cas :

Assumer est une entreprise, qui propose des produits classiques d'assurance à destination de clients particuliers ou professionnels.
Il s'agit d'une PME (Petite Moyenne entreprise) comprenant 20 collaborateurs au siège, et de 5 à 10 collaborateurs répartis sur les 15 agences sur toute la France.

Le siège est composé de quatre services, la DSI, le service Finance et Comptabilité, le service Ressources Humaines, et le service assurance. Tous les serveurs de l'entreprise sont stockés chez IT Cloud, l'entreprise possède actuellement une ferme de 12 serveurs ayant une capacité d'extension jusqu'à 20 en cas de nécessité.

À la suite de la mise en place du télétravail, nous devons proposer une solution d'infrastructure réseau qui permettrait à tous les collaborateurs de se connecter et travailler aussi bien en distanciels qu'en présentiel sur sites, sans que cela entraine une baisse de la performance et donc de productivité. Vous pouvez retrouver l'architecture d'existante en annexe 1.

Justification des choix :

Une proposition de la future architecture disponible en annexe 2.

En ce qui concerne l'adressage IP, nous partirons sur :

- Du 10.100.100.1-15/24 pour les serveurs.
- Pour le siège 10.10.x.x / 24 en fonction des Vlan
- 10.10.x.253-254 /24 pour le stack des deux switches.
- Enfin pour les agences 10.1.x.x /24 en fonction de chaque agence 10.1.x.254 /24 pour le switch.

Nous partirons sur ces réseaux qui chacun permettent 254 hôtes, étant simple pour la gestion du réseau, et nous remarquerons une logique au niveau des IP. De plus, il pourra alors avoir une perspective d'évolution sans devoir refaire toute l'infrastructure réseau. Ces réseaux seront bien évidement sécurisés par le principe des Vlan. Un vlan est un réseau local virtuel, il en existe 3 types qui sont en rapport avec leurs actions sur les couches du modèle OSI :

Vlan de niveau 1(aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.

VLAN de niveau 2 (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :

- Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
- Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

Dans notre cas, la structure serait un Vlan par service et par imprimante au siège donc 8 Vlan (Vlan-AssuBusines-2, Vlan-AssuPart-3, Vlan-ComptaCli-4, Vlan-DSI-5, Vlan-ComptaCola-6, Vlan-RH-7, Vlan-Imp1-8, Vlan-Imp1-9) et aussi un Vlan par agence. Cette architecture sera plus simple pour gérer les ACL (Access Control List) et pour gérer la communication entre les différents services et on autorisera certaines IP à communiquer avec d'autres déjà autorisées.

On partira sur du Vlan de niveau 1 car il permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre, offrir les avantages suivants, plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs. Un gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées, également une réduction de la diffusion du trafic sur le réseau.

Mais évidemment, ce choix présente ces failles comme il suffit de prendre la prise d'alimentation du PC proche de celui-ci et nous pouvons être connecter sur un autre Vlan, c'est pour cela que les espaces dans le siège précisément doivent etre bien définit et séparé.

Nous décidons de mettre en place de la haute disponibilité, donc de garantir la continuité des services. Cette mise en place limite les points de rupture de l'infrastructure (les SPOFs = Single Point Of Failure). Par conséquent, pour le siège, dans le rack, il faudra doubler tout le matériel donc deux FAI, deux pares-feux, deux switches. Puis, il faudra faire un cluster de pares-feux, c'est-à-dire mettre les pares-feux dans une grappe il y aura alors un firewall maitre et l'autre sera un firewall esclave. Le maitre sera alors l'actif et l'esclave est alors passif en attendant que le maitre soit défaillant.

Pour les switches, on va les relier avec deux câbles stack. De manière virtuelle, un stack de plusieurs switches se comportant comme un seul et même switch. Ainsi, l'ensemble des switches ne possède qu'une unique adresse IP, et une seule configuration. En plus de simplifier le management (une seule IP, une seule config, une seule supervision), la mise en stack améliore la disponibilité, la performance, et la fiabilité du réseau.

Néanmoins, pour les agences, nous n'allons pas mettre en place de HA mais juste doubler les FAI. Car nous estimons que si un switch ou un firewall soit défaillant, ce n'est pas trop grave. Il faudra alors prévoir 2, 3 switches et firewall de spare.

En ce qui concerne le routage et les liens télécom,

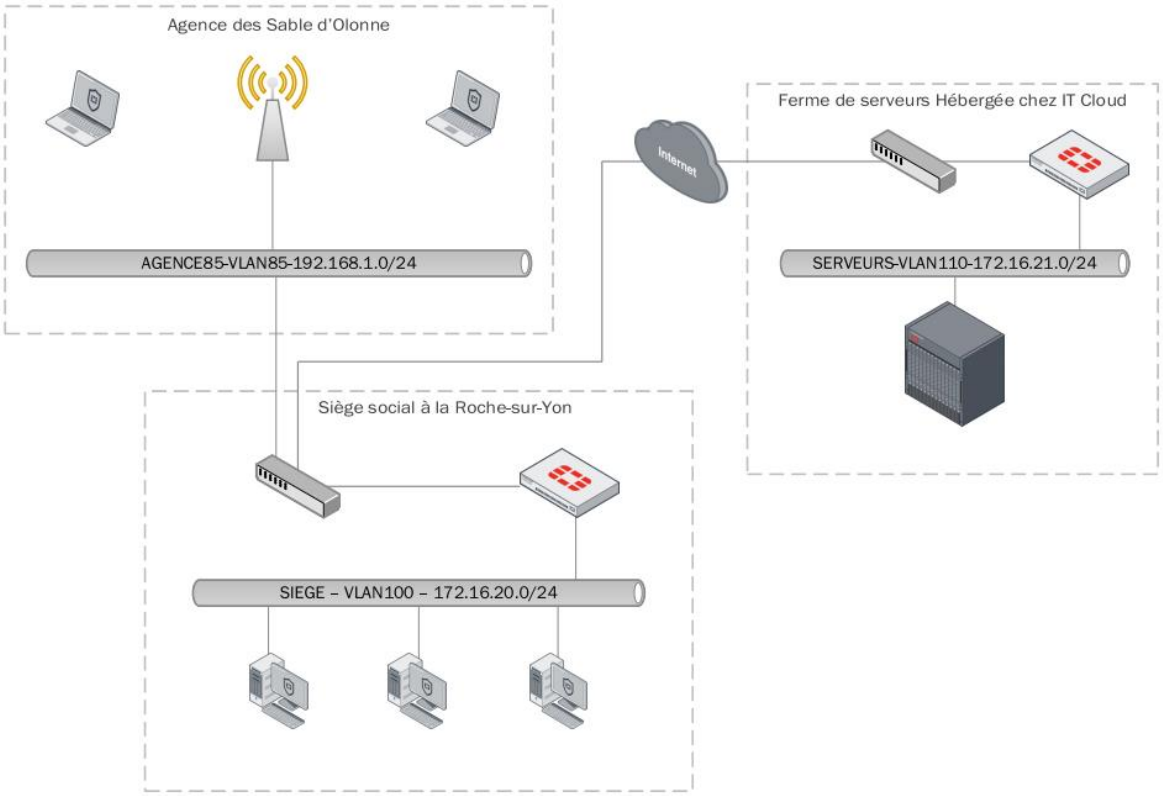
- pour le siège, on aura deux FAI (Orange et Bouygues) avec un lien 1Gbps et un deuxième de secours dégressif avec 200Mbps.
- pour les agences 2 FAI Orange et Bouygues avec un lien 1Gbps et un deuxième de secours dégressif avec 200Mbps (box 4G).
- Les deux sont des liens fibrés, nous pensons qu'il ne répondrait pas au besoin d'avoir de ligne dédiée ou ligne MPLS.
  Les agences ne pointent plus sur le siège mais directement sur IT Cloud pour une meilleure disponibilité.

En ce qui concerne le VPN, qui est un système permettant de créer un lien direct entre des ordinateurs distants, ressources, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics et dans notre cas, on en utilise de deux types le VPN :

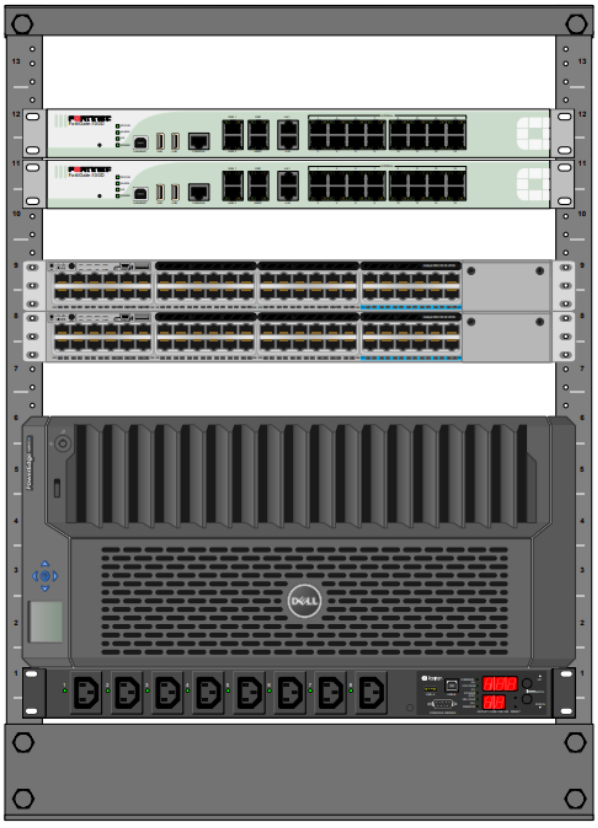
- Pour les collaborateurs sur site, ils utiliseront un VPN IP Sec, créant une ligne isolée entre les deux firewall, cette connexion est sécurisée et stable. (Annexe n°2 (architecture agence))
- Nous avons aussi le VPN SSL utilisé pour les collaborateurs en télétravail. Cela permettra une connexion directe sur le firewall de IT Cloud pour accéder aux ressources. Néanmoins pour des raisons de sécurité, il faudra mettre en place le protocole LDAP pour sécuriser cette connexion (avec un système d'authentification). Les utilisateurs pourront aussi utiliser l'application Forticlient pour cette connexion. –(Annexe n°2 (télétravail))

Pour les pare-feux, on choisit des Fortinet Fortigate-100D, qui est un firewall permettant la gestion des Vlan et aussi le VPN (énoncé ci-dessus), possédant aussi une interface graphique agréable et simple d'administration.

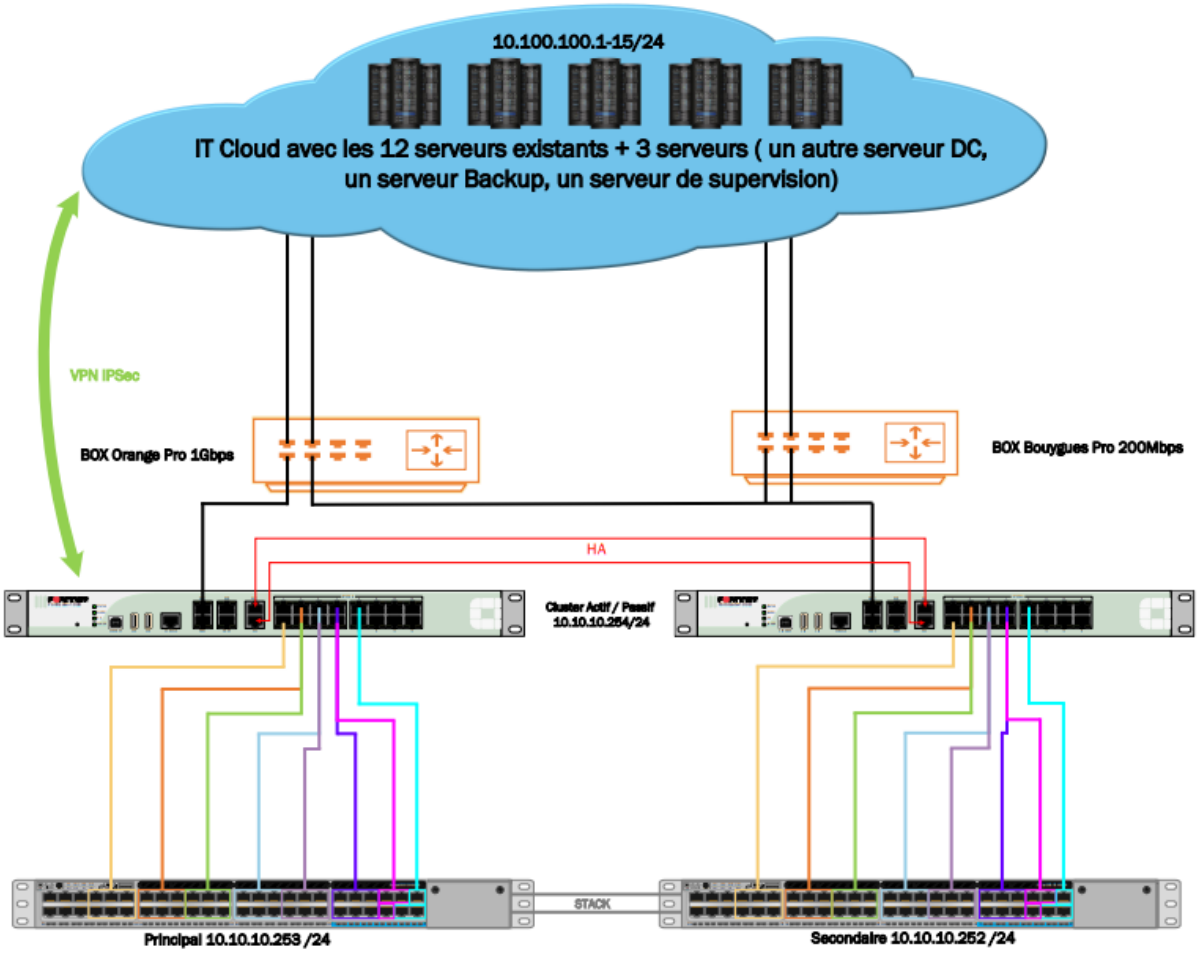
Annexe n°1



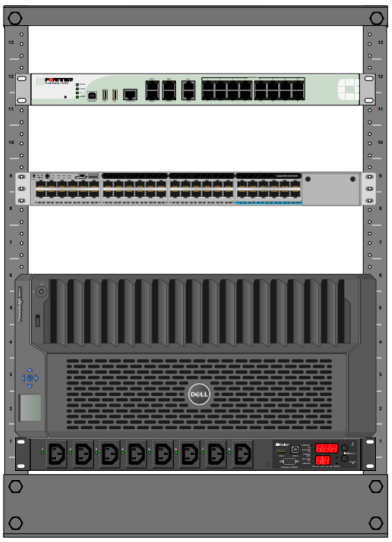
Annexe n°2 (rack serveur siège)



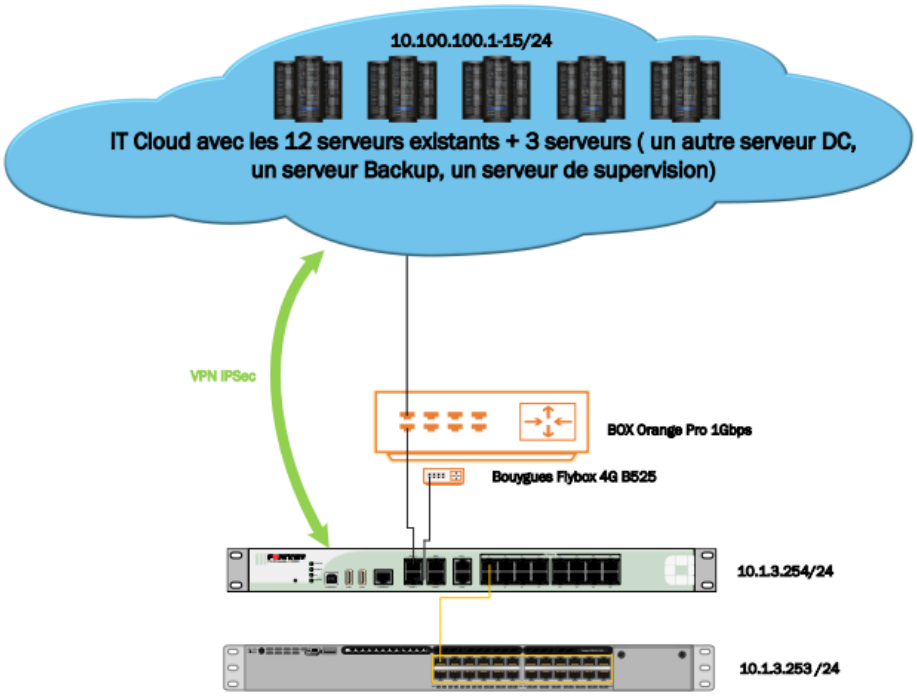
Annexe n°3 (architecture siège)

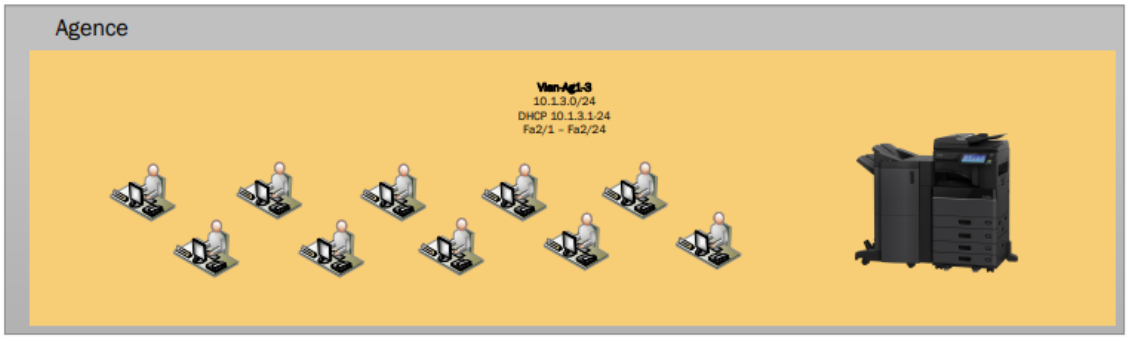


Annexe n°4 (rack serveur agences)



Annexe n°5 (architecture agence)





Annexe n°6 (télétravail)