TP architecture réseau sécurisée

Nyouri Kaoutar & Tabani Kenza

I. Choix des équipements :

Pour répondre aux besoins de l'entreprise, nous avons besoin de plusieurs équipements de réseau :

Des commutateurs (switches) pour connecter les différents appareils entre eux et permettre leur communication.

Un routeur pour acheminer le trafic entre les différents réseaux et vers Internet.

Un firewall pour protéger le réseau contre les attaques extérieures.

Voici les équipements qu'on propose :

-Commutateurs : nous allons utiliser des commutateurs Gigabit Ethernet pour pouvoir profiter de la vitesse de transmission des cartes réseaux Gigabit de nos serveurs. Nous allons en acheter 3, pour chacun des bâtiments, afin de connecter tous les appareils. Nous avons choisi 3 commutateurs Cisco SG350-28P, au prix de 1 000 € l'unité. Ces commutateurs sont Gigabit Ethernet et permettent de connecter tous les appareils entre eux dans chaque bâtiment. Ils sont également équipés de ports PoE, ce qui permet de fournir de l'énergie aux appareils connectés par le biais du câblage Ethernet.

-Routeur : nous allons utiliser un routeur Gigabit Ethernet pour pouvoir acheminer le trafic vers Internet et entre les différents réseaux. Nous allons le placer dans le local technique n°1, où arrive la connexion Internet par fibre optique. Nous avons choisi un routeur Cisco RV340W, au prix de 250 €. Ce routeur est Gigabit Ethernet et permet d'acheminer le trafic entre les différents réseaux et vers Internet. Il est équipé de ports WAN et LAN, ce qui permet de le relier à la connexion Internet par fibre optique et aux commutateurs des bâtiments 1 et 2.

Firewall : Nous allons le placer dans le local technique n°1, afin de sécuriser l'accès à Internet et aux différents réseaux. Nous avons choisi un firewall Cisco ASA 5506-X, au prix de 500 €. Ce firewall permet de protéger le réseau contre les attaques extérieures et de contrôler l'accès à Internet. Il est relié au routeur par un câble de catégorie 6 et est configuré pour accepter ou bloquer le trafic selon les règles de sécurité définies.

Voici les références exactes des équipements qu'on a choisis :

Commutateurs : Cisco SG350-28P (3 unités)
Routeur : Cisco RV340W
Firewall : Cisco ASA 5506-X
Le budget total de ces équipements est de 3 750 €, ce qui est inférieur au budget de 15 000 € dont nous disposons

II. Conception de l'architecture réseau :

Schéma physique :

Nous avons choisi d'utiliser des câbles de catégorie 6 pour relier les locaux techniques entre eux et pour connecter les appareils dans chaque bâtiment. Les câbles de catégorie 6 sont capables de transmettre des données à des vitesses allant jusqu'à 10 Gbit/s sur des distances

allant jusqu'à 100 mètres. Ils sont également blindés, ce qui les protège contre les interférences électromagnétiques et leur permet de maintenir une qualité de signal élevée.

Dans chaque bâtiment, nous avons installé un commutateur pour connecter tous les appareils entre eux. Le commutateur du bâtiment 1 connecte les appareils du département marketing et du département production, tandis que le commutateur du bâtiment 2 connecte les appareils du département développement. Chaque commutateur est équipé de ports Gigabit Ethernet, ce qui permet de profiter de la vitesse de transmission des cartes réseaux Gigabit de nos serveurs.

Les commutateurs du bâtiment 1 et du bâtiment 2 sont reliés entre eux par un câble de catégorie 6, afin de permettre la communication entre les appareils des différents départements.

Nous avons installé un routeur dans le local technique n°1, qui est le cœur de notre réseau. Le routeur est relié aux commutateurs du bâtiment 1 et du bâtiment 2 par des câbles de catégorie 6. Il est également relié à la connexion Internet par fibre optique. Le routeur est capable de gérer le trafic entre les différents réseaux et de le diriger vers Internet ou vers d'autres destinations.

Nous avons installé un firewall dans le local technique n°1, qui est relié au routeur par un câble de catégorie 6. Le firewall est configuré pour protéger le réseau contre les attaques extérieures et pour contrôler l'accès à Internet. Il bloque ou autorise le trafic selon les règles de sécurité définies.Voici le schéma de l'architecture physique de notre réseau :

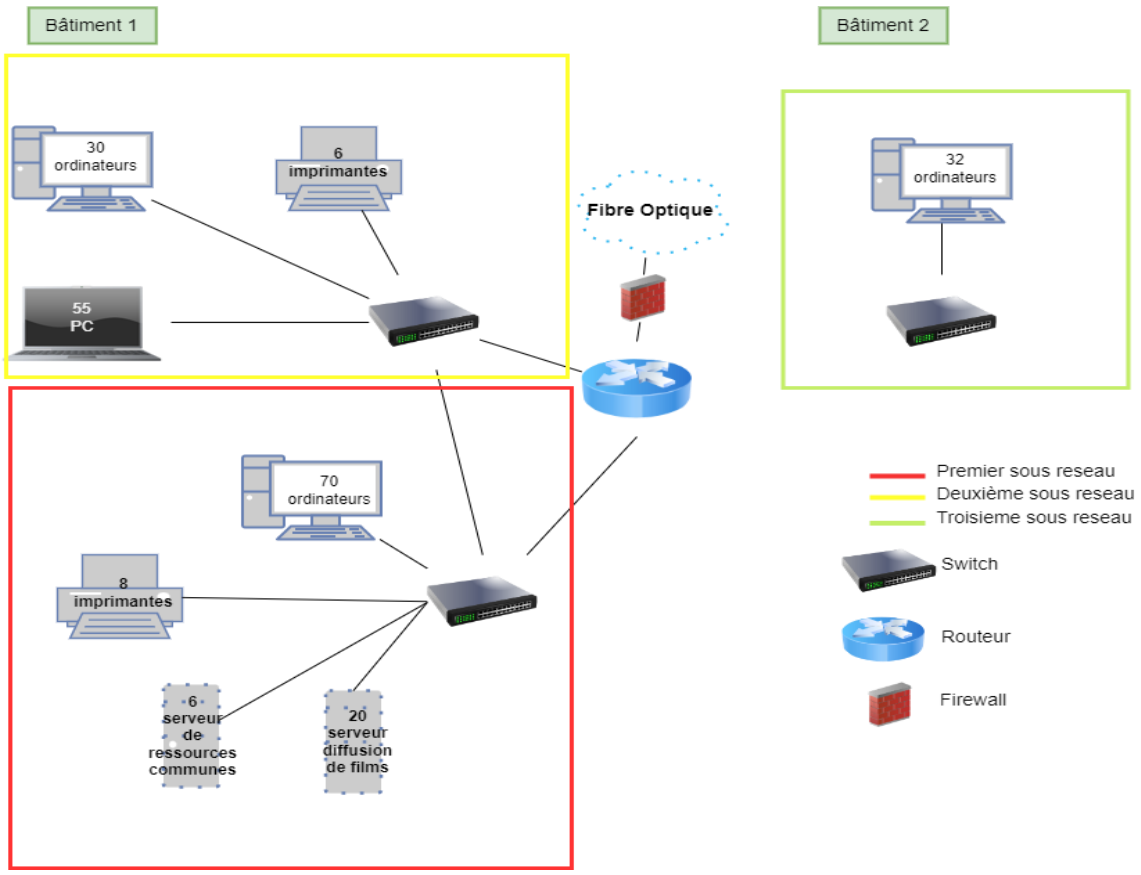
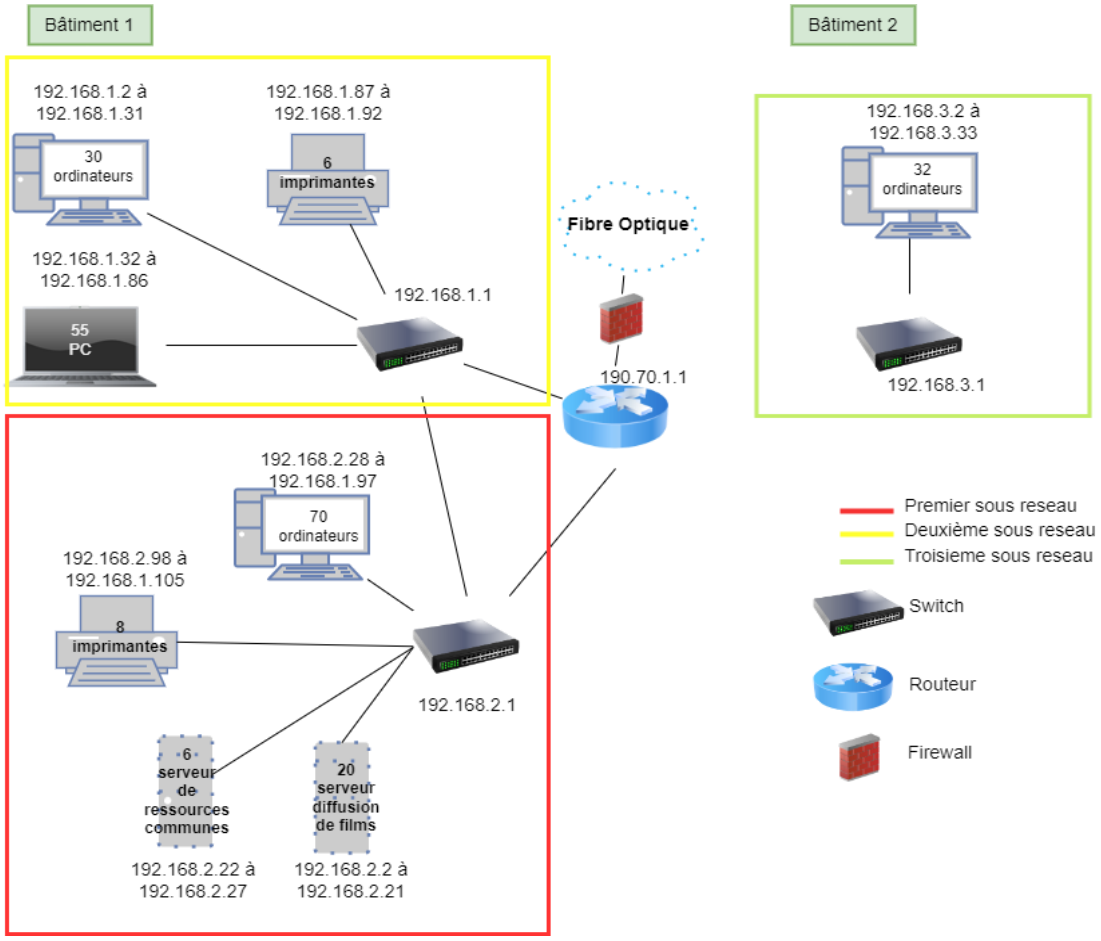


Schéma logique :

Notre réseau est organisé en trois sous-réseaux distincts, correspondant aux départements Marketing, Production et Développement. Chaque sous-réseau est connecté à un commutateur, qui permet de connecter les appareils de chaque département entre eux. Tous les commutateurs

sont à leur tour connectés au routeur, qui permet de connecter notre réseau à Internet. Le routeur est également équipé d'un firewall, qui protège le réseau contre les menaces en ligne.



Le préfixe de réseau 190.70.1.0/27 attribué par le fournisseur d'accès Internet est utilisé pour les adresses IP publiques de notre réseau. Les adresses IP publiques sont utilisées par les routeurs pour connecter notre réseau à Internet. Les commutateurs, en revanche, ont des adresses IP privées, qui appartiennent à la plage 192.168.x.x. Les adresses IP privées sont utilisées uniquement dans notre réseau local, et ne sont pas accessibles depuis Internet, et de cette façon, on protège notre réseau contre les menaces en ligne.

Routeur	Département Marketing	Département Production	Développement :
190.70.1.1	**Commutateur :** 192.168.1.1 **Postes de travail :** 192.168.1.2 à 192.168.1.31 **Ordinateurs portables :** 192.168.1.32 à 192.168.1.86 **Imprimantes :** 192.168.1.87 à 192.168.1.92	**Commutateur :** 192.168.2.1 **Serveurs de diffusion de films :** 192.168.2.2 à 192.168.2.21 **Serveurs de ressources communes :** 192.168.2.22 à 192.168.2.27 **Postes de travail :** 192.168.2.28 à 192.168.2.97 **Imprimantes :** 192.168.2.98 à 192.168.2.105	**Commutateur :** 192.168.3.1 **Postes de travail :** 192.168.3.2 à 192.168.3.33

III. Justification des choix et évaluation de l'évolutivité de la solution :

Pour justifier nos choix, voici les principaux arguments :

-Utilisation de commutateurs pour chaque département : en utilisant un commutateur pour chaque département, on peut créer des segments de réseau dédiés qui sont indépendants les uns des autres. Cela permet de séparer le trafic généré par chaque département et d'éviter qu'il n'affecte le fonctionnement du reste du réseau.

-Utilisation de routeurs pour connecter les différents segments de réseau : cela permet de créer un réseau étendu qui permet à tous les appareils de communiquer entre eux, quelle que soit leur localisation. Le routeur permet également de connecter le réseau local à Internet et de protéger le réseau contre les menaces en ligne.

-Utilisation de câblage en paire torsadée de catégorie 6 : ce type de câblage est adapté à des débits de transmission de données allant jusqu'à 10 Gbit/s et peut être utilisé sur de longues distances. Il est donc adapté à notre réseau, qui doit couvrir deux bâtiments de grande taille.

-Utilisation d'adresses IP privées pour les commutateurs : en utilisant des adresses IP privées pour les commutateurs, on empêche les appareils du réseau de communiquer directement avec Internet et protéger ainsi notre réseau contre les menaces en ligne.

-Utilisation d'une connectivité Internet par fibre optique, qui est une solution très performante et évolutive. Cela nous permet de disposer de débits élevés, qui nous permettront de connecter de nombreux appareils

-En ce qui concerne le matériel, nous avons choisi le routeur Cisco RV340W pour sa qualité, sa vitesse de transmission de données, ses fonctionnalités de sécurité avancées et sa compatibilité avec les protocoles de seau courants. Le prix de ce routeur est abordable et convient à notre budget. De plus, il est évolutif et peut être facilement mis à niveau au fur et à mesure de l'ajout de nouveaux appareils ou de l'augmentation de la charge de trafic sur le réseau.

En ce qui concerne l'évolutivité de notre solution, voici quelques points à considérer :

Pour assurer la tolérance aux pannes, nous avons également prévu l'utilisation de serveurs de ressources communes dans le département Production. Ces serveurs sont chargés de stocker et de fournir les ressources communes (messagerie, web intranet, etc.) aux autres appareils du réseau, de sorte que leur indisponibilité ne mette pas en péril le fonctionnement du reste du réseau.

Pour ajouter de nouveaux appareils ou de nouveaux départements, il est recommandé de disposer de suffisamment de ports disponibles sur les commutateurs et le routeur. Pour notre solution, nous avons choisi des commutateurs et un routeur avec un grand nombre de ports, ce qui nous permet d'étendre notre réseau sans avoir à changer d'équipement.

Il est également important de s'assurer que le matériel choisi est compatible avec les standards de l'industrie et est capable de prendre en charge les nouvelles technologies. Les commutateurs et le routeur que nous avons sélectionnés sont tous de marques reconnues pour leur qualité et leur fiabilité, et sont capables de prendre en charge les normes de l'industrie en matière de câblage et de communication réseau.

En résumé, notre architecture de réseau a été conçue de manière à être sécurisée, évolutive et adaptée à notre budget. Nous avons utilisé du matériel de qualité et adapté aux besoins de l'entreprise, et avons pris en compte les contraintes et conditions imposées pour assurer le bon fonctionnement du réseau.