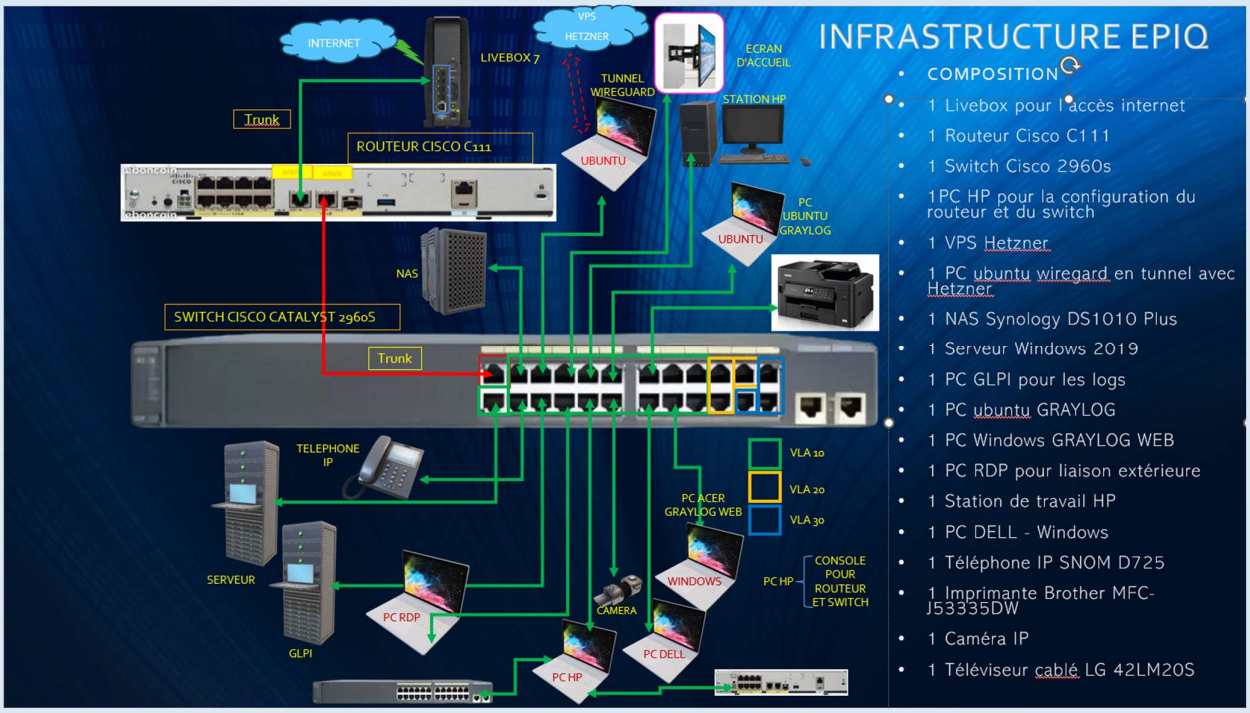
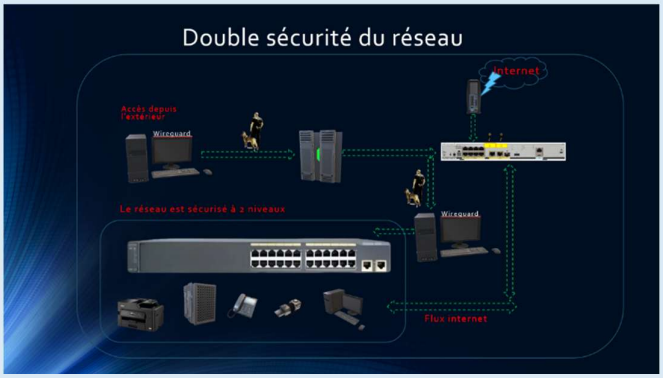
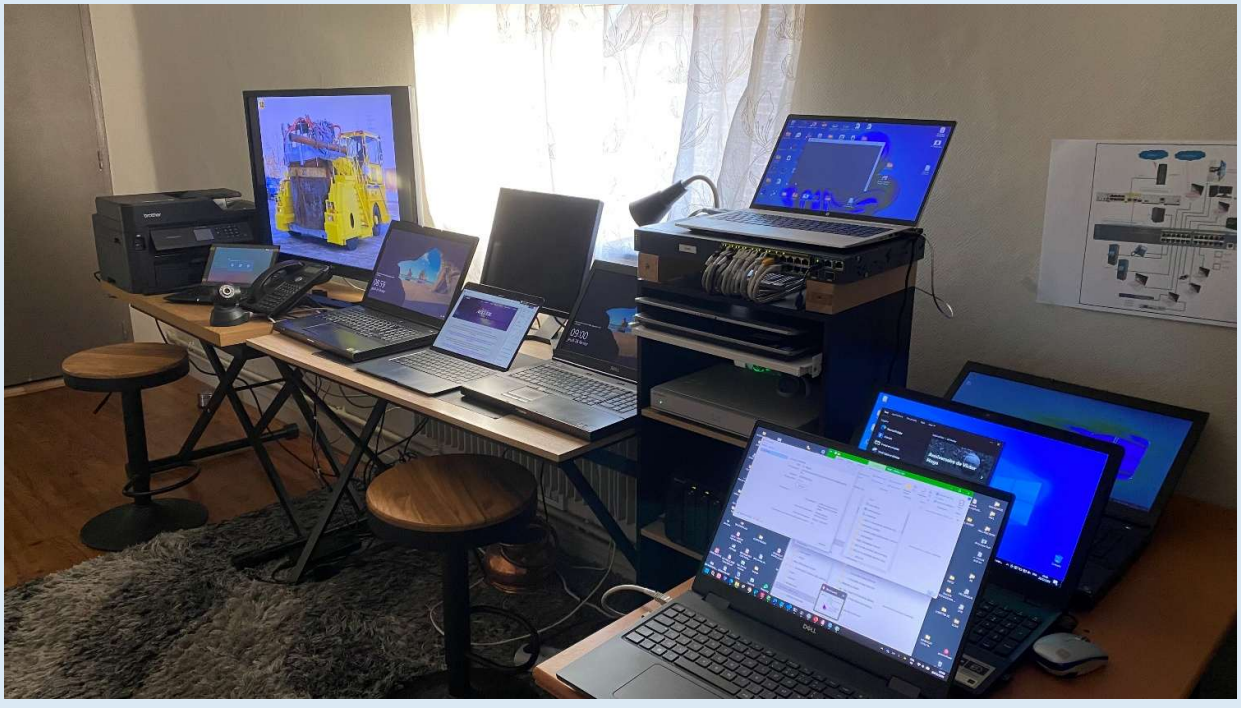
MON PROJET EN ENTREPRISE







1. Le cahier des charges :

Réalisation d'une infrastructure réseau complète. Le cahier des charges me laissait le choix du matériel et des logiciels. L'infrastructure devait utiliser : des serveurs, des PC et station de travail, un NAS, une caméra, une imprimante et un téléviseur connecté. Le réseau pouvait être accessible depuis l'extérieur en 4G par exemple, sans compromettre la sécurité. Je devais pouvoir remonter les logs et les filtrer pour en faire une gestion et les exporter sur Excel pour une analyse.

2. Les préparatifs

Pour cela, j'ai donc commencé par établir une liste de tâches à accomplir :

- **La liste du matériel**
- **La liste des logiciels**
- **Le schéma de l'infrastructure avec tous les équipements du cahier des charges**
- **La définition de la sécurité du réseau (VPN)**

J'ai choisi CISCO car je connaissais ce matériel.

- **J'ai donc pris un routeur CISCO C1111 et un switch Catalyst 2960s**
- **Et pour l'accès extérieur sécurisé j'ai choisi un VPS de chez Hetzner**

Pour les logiciels, j'ai choisi :

- **Windows Server 2019**
- **Syslog**
- **Arden AD**
- **Graylog**

- **J'ai fait approvisionner le matériel,**
- **Téléchargé les logiciels,**
- **Réalisé le schéma de l'installation avec l'attribution des ports pour chaque appareil**

3. La réalisation :

A la réception du matériel, j'ai procédé à :

- **La réalisation du câblage,**
- **Le repérage des connexions et**
- **La mise au propre**

J'ai pu alors me consacrer à la configuration du VPS, du Routeur et du Switch

Sur le routeur : ----------

- **Il est connecté à une Livebox 7 (pour donner l'accès à internet au routeur)**
- **C'est maintenant le routeur qui va attribuer les adresse IP aux équipements du réseau**
- **J'ai séparé en 3 zones/ VLAN 10, réseau principal**
- **VLAN20 réseau secondaire et**
- **VLAN30 réseau invité**
- **J'ai ensuite :**
- **Paramétré le VLAN30 pour accéder à internet seulement mais pas aux VLANs**
- **Attribué des adresses IP fixes pour les accès extérieurs**
- **Spécifié un accès en SSH sécurisé uniquement**
- **Créé une route pour envoyer le trafic venant du VPS Hetzner vers le PC Tunnel Wireguard**

Sur le Switch : ----------

- **J'ai procédé aux actions suivantes**
- **Déclaration les VLANs 10, 20 et 30**
- **Configuration du trunk vers le routeur auquel j'ai alloué les VLAN**
- **Configuration des plages des ports pour les 3 VLANs**
- **Activation SSH pour la sécurité**

Je me suis ensuite consacré à la sécurité du réseau.

Sur le VPS de chez Hetzner : ----------

- **J'ai procédé aux actions suivantes**
- **Installation du VPS avec Ubuntu**
- **Paramétrage du VPN Wireguard (Hetzner) qui m'a donné la clé publique et la clé privée**
- **Paramétrage des règles du firewall pour un accès sécurisé depuis l'extérieur**

Sur le PC Tunnel Wireguard ----------

- **J'ai procédé aux actions suivantes**
- **Installation de Ubuntu et configuré Wireguard qui m'a donné une clé publique et une clé privée**
- **Echange des clés entre le VPS et le PC Ubuntu Wireguard pour créer le tunnel**
- **Tout le trafic VPS passe par Wireguard**

J'ai ensuite fait des tests pour vérifier que le trafic passe bien par le tunnel.
Par exemple débranchement du câble réseau du PC wireguard pour vérifier que l'accès venant du VPS ne passait pas.

4. Le serveur Principal et le serveur GLPI

Sur le Serveur Principal ----------

J'ai installé :

- **Windows Server 20219**
- **Syslog**
- **Harden AD pour les GPO**

J'ai ensuite :
Déclaré son adresse IP fixe
Défini le domaine
Mis en place l'Active Directory

Et pour les GPOs, j'ai

- **Déclaré plusieurs groupes et plusieurs personnes dans chaque groupe**
- **Attribué des droits pour l'accès à certains dossiers en fonction des groupes auxquels ils appartiennent**
- **Tous les groupes ont un lien direct (raccourci) vers le server GLPI via une interface Web**

J'ai vérifié le bon fonctionnement de Syslog

Le Serveur GLPI----------

J'ai installé

- **Windows Server 2019**
- **GLPI**
- **WAMP**

J'ai d'abord lié le serveur GLPI au domaine du serveur principal, puis
Paramétré Wamp\Apache pour donner un accès localhost à tous les utilisateurs du réseau,
Déclaré l'ensemble des groupes et des utilisateurs comme ceux du serveur principal
Paramétré des rôles aux utilisateurs pour les autoriser à créer des tickets

Ensuite j'ai procédé à des tests de création de tickets à partir de différents utilisateurs.

Dans le cahier des charges, je devais créer des logs des déconnexions physiques sur le switch ou les équipements.

Pour cela, j'ai utilisé un serveur Graylog car Syslog ne peut pas récupérer directement ces logs physiques.

5. Le serveur Garylog

Pour le Serveur Graylog : ----------
J'ai utilisé un autre PC sur lequel j'ai installé

- **Ubuntu**
- **Graylog qui inclus:**
- **Graylog server,**
- **Elasticsearch**
- **MongoDB**

Je me suis servi de la procédure d'installation du site Graylog

Depuis un autre PC sur le réseau, j'ai testé la connexion à la page web de graylog

Pour que graylog puisse recevoir les logs de déconnexion du switch, il a fallu:

Sur le Switch : ----------

- **Déclarer une adresse IP fixe du switch pour l'envoi des logs dans le serveur graylog**
- **Déclarer la route vers l'IP du serveur graylog**

Ensuite créer un input sur graylog en Syslog UDP et configurer plusieurs filtres,

- **Sans filtre (je vois tous les logs du switch)**
- **Je ne filtre que "Changed to up & changed to down"**
- **Je ne filtre que "Changed to down"**

Puis l'export des logs sur un tableau excel

6. L'accès Distant

Un autre point demandé au cahier des charges était l'accès sécurisé depuis l'extérieur :

- **Au NAS**
- **A la caméra IP**
- **Au téléphone IP**

Pour cela, j'ai installé Wireguard Windows sur un autre PC
A la configuration, il m'a donné sa clé publique et sa clé privée
Puis sur le VPS Hetzner, j'ai ajouté ce PC dans le Wireguard et
Paramétré les règles du firewall pour accéder à ces 3 appareils

J'ai aussi saisi le nom de ces appareils avec leur adresse IP dans le fichier hosts de ce PC.
C'est plus simple de mettre le nom que l'adresse IP dans l'explorateur windows pour l'accès à distance.

Le dernier point demandé au cahier des charges était l'accès en RDP à la station de travail
Pour cela, j'ai configuré la station de travail pour qu'elle accepte le bureau à distance, puis

Paramétré la règle du firewall du VPS Hetzner pour accéder à ce PC

J'ai fait le test en 4G avec le PC sur lequel wireguard était installé et actif et j'avais bien l'accès au PC de travail

Et pour les besoins de mon exposé, à partir de ce PC de travail, j'ai paramétré des liaisons RDP vers:

- **Le Serveur principal**
- **Le serveur GLPI**
- **Le serveur Graylog**
- **La console CISCO (Putty du Routeur et du Switch)**

7. Backup documentation et tests

J'ai fait des backups au fur et à mesure et comme tout fonctionne correctement j'ai fait un backup final de:

- **VPS Hetzner**
- **Routeur**
- **Switch**
- **Ubuntu Wireguard**
- **Ubuntu Graylog**
- **Serveur Principal**
- **Serveur GLPI**

Le dossier d'utilisation et de configuration : ----------

Dans ce dossier, j'ai mis :

- **La présentation générale**
- **La liste et la référence des équipements**
- **Le schéma de l'infrastructure**
- **Le tableau d'adressage des ports du switch**
- **La liste des logiciels**
- **La configuration du VPS Hetzner**
- **La configuration du routeur**
- **La configuration du switch**
- **La configuration du Wireguard Ubuntu**
- **La configuration du wireguard PC distant**
- **La procédure d'installation et le paramétrage de graylog**
- **La procédure d'exportation Excel depuis graylog web**
- **La liste des groupes et des utilisateurs avec leurs droits**
- **La procédure d'édition et de gestion de tickets**

Les Tests pour dépannage : ----------

Mon tuteur a créé de nombreuses pannes sur le réseau pour vérifier que je pouvais réparer rapidement :
Déconnexions de câbles coté Switch et coté équipement
Mauvais loggings et mauvais mots de passe
Equipement éteint ou en veille
Suppression de disque sur le NAS
Papier sur imprimante bloqué
Objectif de la caméra bouché
Appel du mauvais numéro sur le téléphone IP
Clavier débranché etc.