# Rapport de Stage – Deuxième Année

Introduction

Dans le cadre de ma deuxième année de formation, j'ai effectué un stage au sein de la CIRISI (Cellule Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information) relevant de l'armée française. Ce stage a été très enrichissant et m'a permis de découvrir de nombreux domaines techniques dans un environnement sécurisé et exigeant.

---

Découverte et travail dans la partie réseau

Lors des deux premières semaines, j'ai été intégré à l'équipe réseau. Cette phase m'a permis d'aborder de nombreuses missions, notamment :

- Gestion du ticketing sur un serveur privé, pour résoudre des incidents réseau et de téléphonie.
- Diagnostic et intervention sur des problèmes de câblage dans les baies de brassage, tests de connectivité (lumières verte/orange sur les switches).
- Transfert de tickets vers d'autres équipes après diagnostic matériel.
- Intervention en téléphonie analogique (RTC), changement de postes et reroutage des connexions.
- Configuration de switches Cisco, y compris des opérations de mise à jour avec gestion de fichiers .bin.
- Création d'un document de commandes réseau pour pallier l'absence de documentation à jour.

Une mission notable a été le remplacement complet d'une baie informatique, avec tri, remplacement et repérage des câbles selon un code couleur précis, installation des switches, et test de connectivité poste par poste.

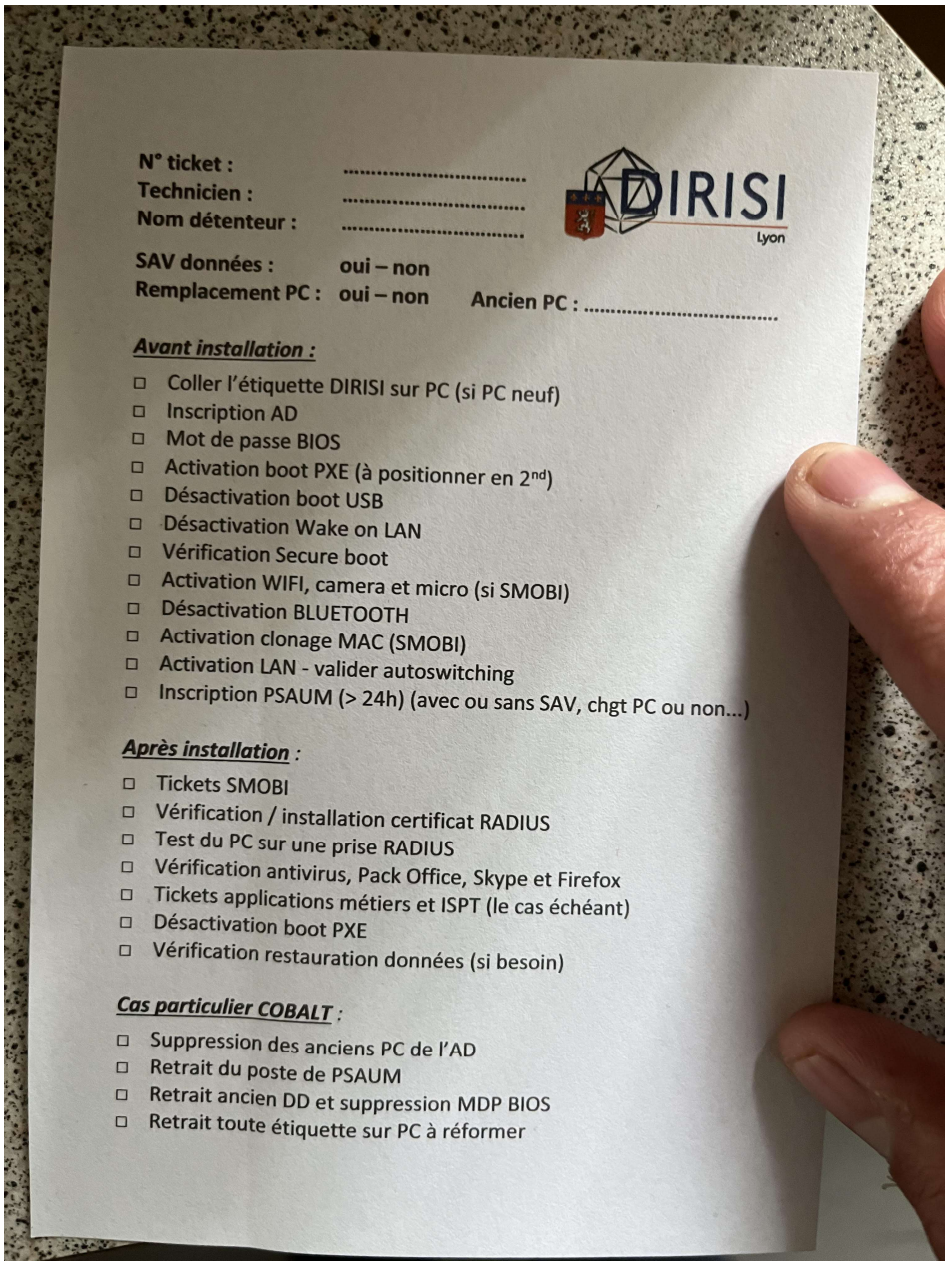
---

Expérience dans la partie système

Les semaines suivantes ont été consacrées à l'équipe système. J'ai pu y explorer les points suivants :

- Réparation de pannes matérielles simulées sur des PC : RAM, disques débranchés, pile BIOS, ports USB désactivés, etc.
- Création d'un Active Directory complet, avec configuration de DNS, DHCP et ADDS.
- Travail sur le déploiement de certificats pour permettre l'accès au réseau dans différents sites (quartier général, 7e RMAT).

- Configuration de postes pour le télétravail : réglages BIOS, installation d'une image système, intégration au réseau Intradef.



N° ticket : .....
Technicien : .....
Nom détenteur : .....

DIRISI
Lyon

SAV données : oui – non
Remplacement PC : oui – non Ancien PC : .....

***Avant installation :***

- ☐ Coller l'étiquette DIRISI sur PC (si PC neuf)
- ☐ Inscription AD
- ☐ Mot de passe BIOS
- ☐ Activation boot PXE (à positionner en 2nd)
- ☐ Désactivation boot USB
- ☐ Désactivation Wake on LAN
- ☐ Vérification Secure boot
- ☐ Activation WIFI, camera et micro (si SMOBI)
- ☐ Désactivation BLUETOOTH
- ☐ Activation clonage MAC (SMOBI)
- ☐ Activation LAN - valider autoswitching
- ☐ Inscription PSAUM (> 24h) (avec ou sans SAV, chgt PC ou non...)

***Après installation :***

- ☐ Tickets SMOBI
- ☐ Vérification / installation certificat RADIUS
- ☐ Test du PC sur une prise RADIUS
- ☐ Vérification antivirus, Pack Office, Skype et Firefox
- ☐ Tickets applications métiers et ISPT (le cas échéant)
- ☐ Désactivation boot PXE
- ☐ Vérification restauration données (si besoin)

***Cas particulier COBALT :***

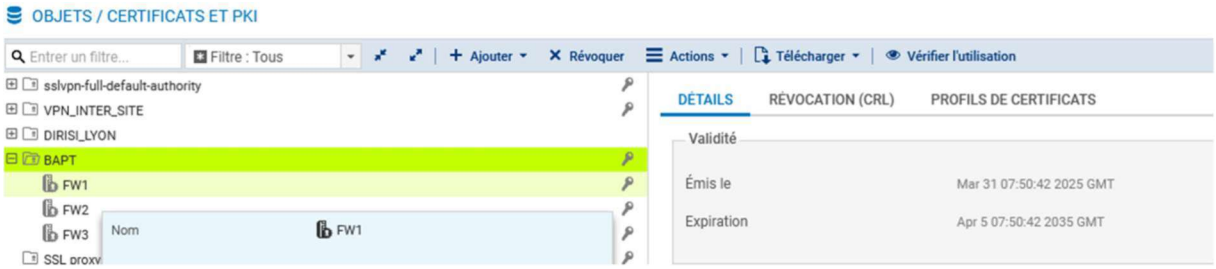
- ☐ Suppression des anciens PC de l'AD
- ☐ Retrait du poste de PSAUM
- ☐ Retrait ancien DD et suppression MDP BIOS
- ☐ Retrait toute étiquette sur PC à réformer

- Audit de sécurité de l'Active Directory avec l'outil PingCastle.
- Apprentissage approfondi du DHCP, de ses mécanismes et de sa gestion dans l'environnement Active Directory.

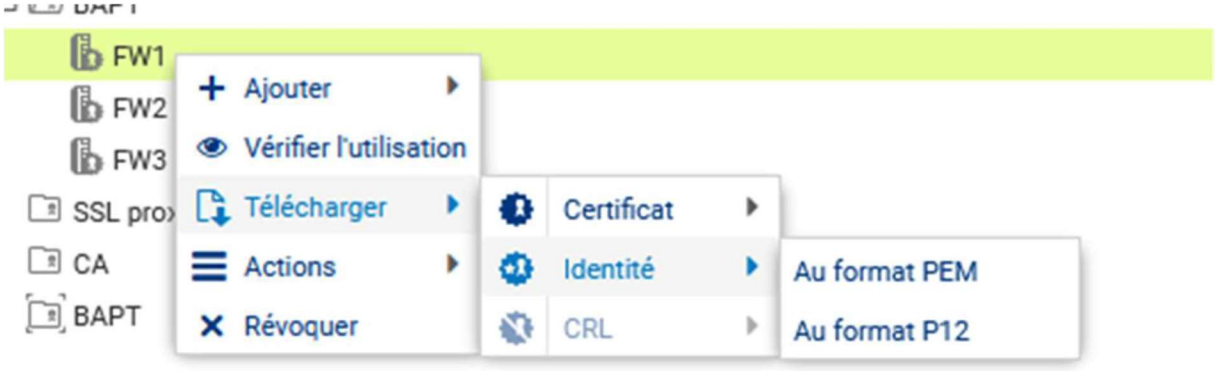
---

Travail avec le CMORD – VPN IPsec

Durant les deux dernières semaines, j'ai travaillé avec le CMORD (relevant de la DIRISI) sur la mise en place d'un VPN IPsec entre trois firewalls :



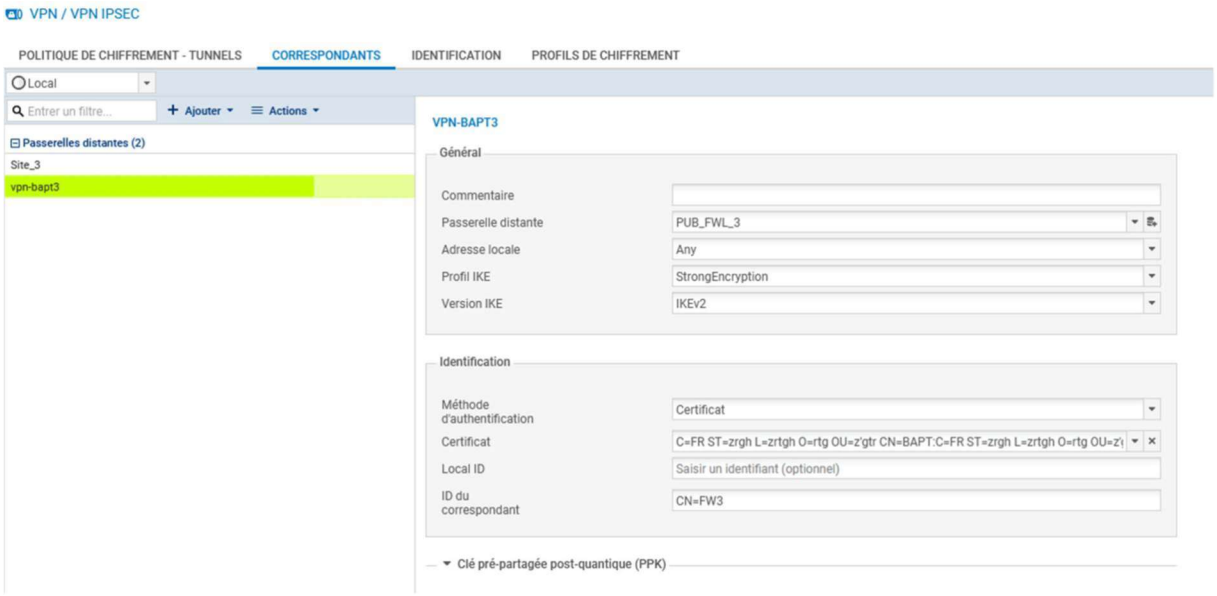

J'ai donc importé les identités serveurs en téléchargeant l'identité au format P12 qui permet d'importer aussi la clé privée.



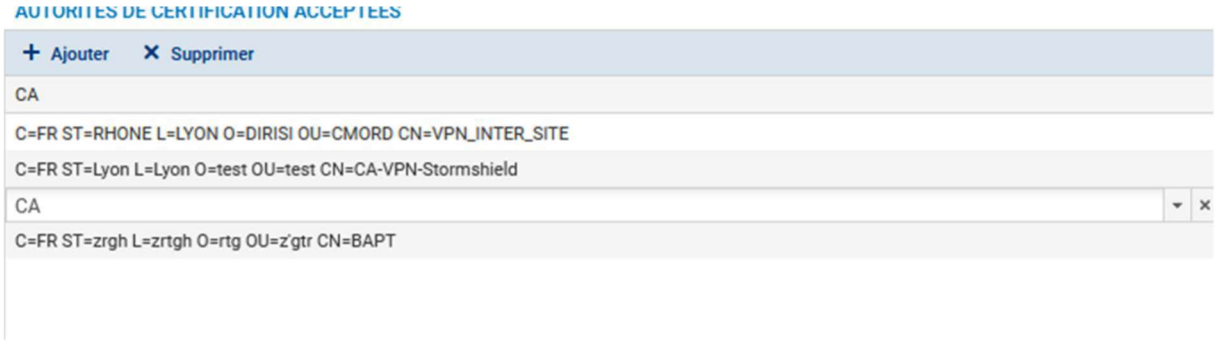

J'ai ensuite ajouté tout ça dans le SMC (Stormshield Management Center) qui va gérer le vpn entre les trois firewalls.


J'ai ensuite créé la topologie vpn.

Après dans chaque firewall il a fallu configurer les correspondant :




L'identification :



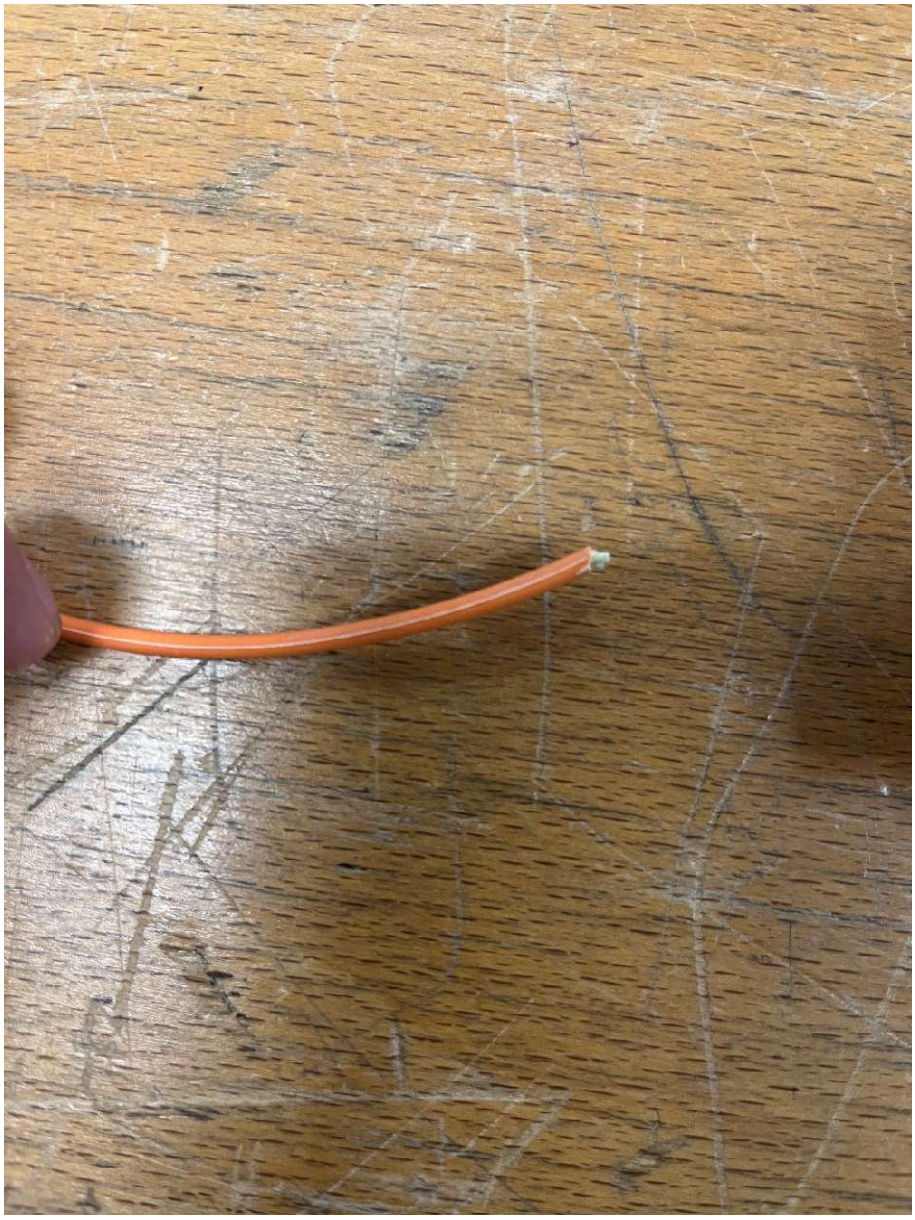

La dernière étape la plus importante est d'importer la CRL du firewall 3 dans les deux autres Firewalls car la CRL (Certificate Revocation List) est un mécanisme de sécurité utilisé pour vérifier Qu'un certificat n'a pas été annulé.
Sans ça le vpn ne peut pas fonctionner.


Voilà le résultat :

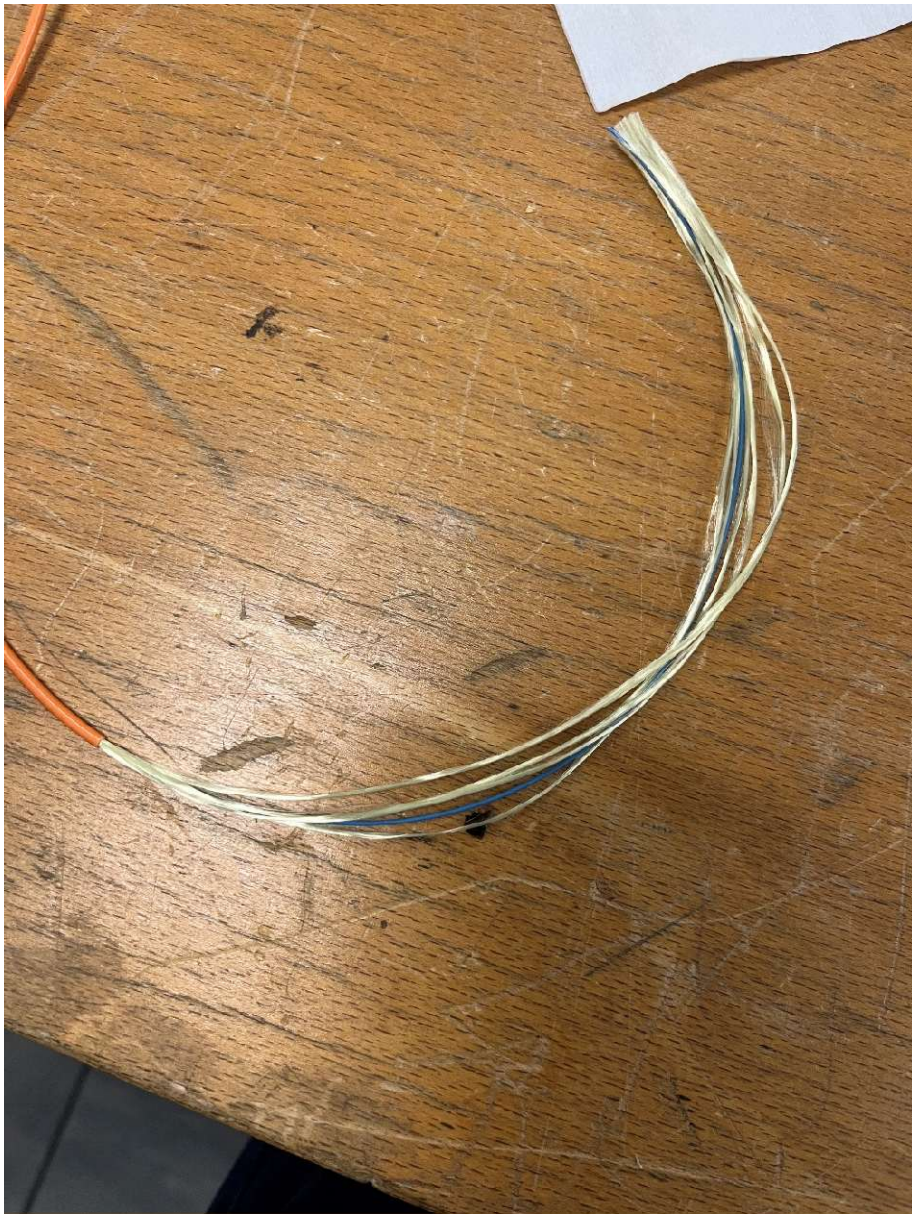
Découverte de la fibre optique

Une autre activité marquante a été la réparation de fibre optique, découverte totale pour moi. Les étapes suivies :

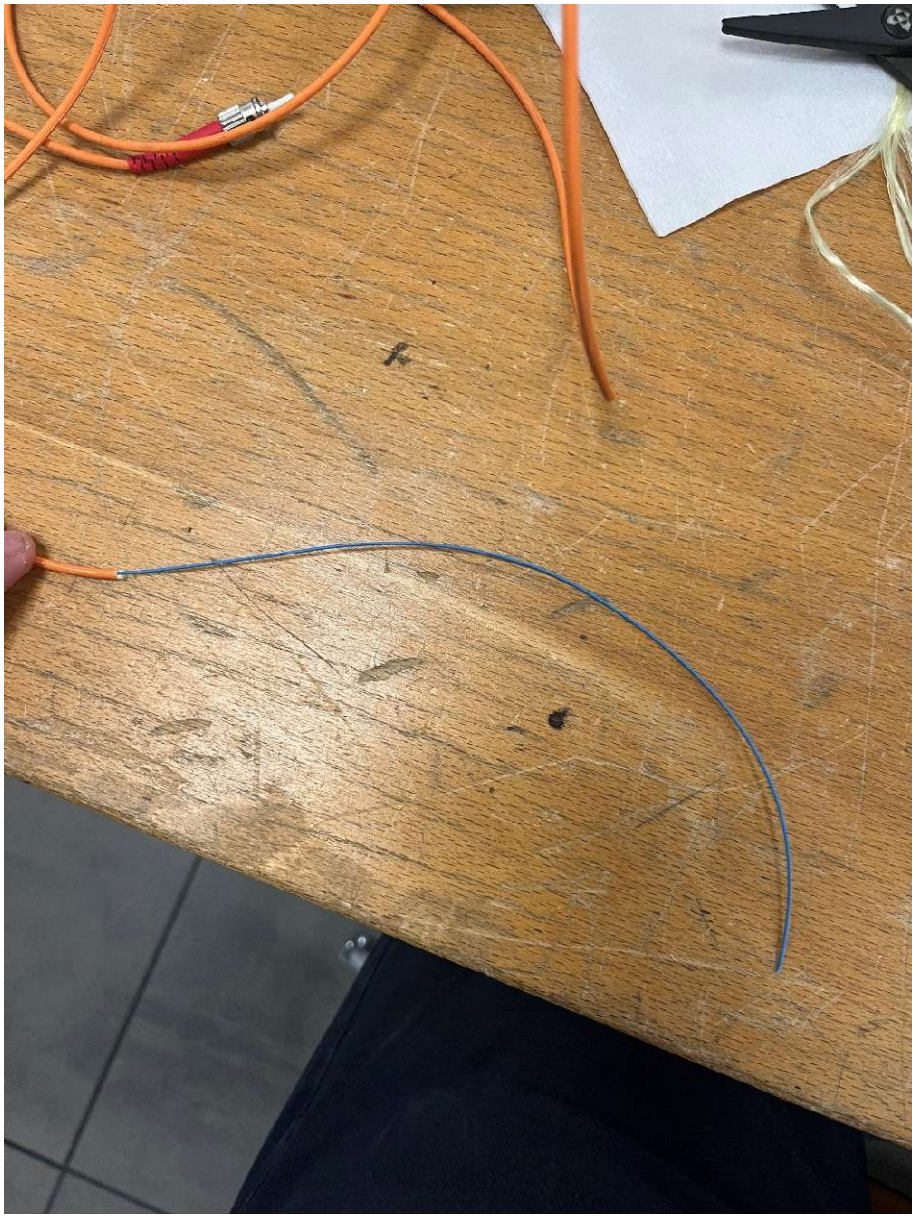
Voilà la fibre de base qui a été arraché



La première étape consiste à enlever la première gaine  et à retiré le kevlar(fils blanc qui servent à protéger la fibre contre les tensions mécaniques)



Voilà le premier résultat

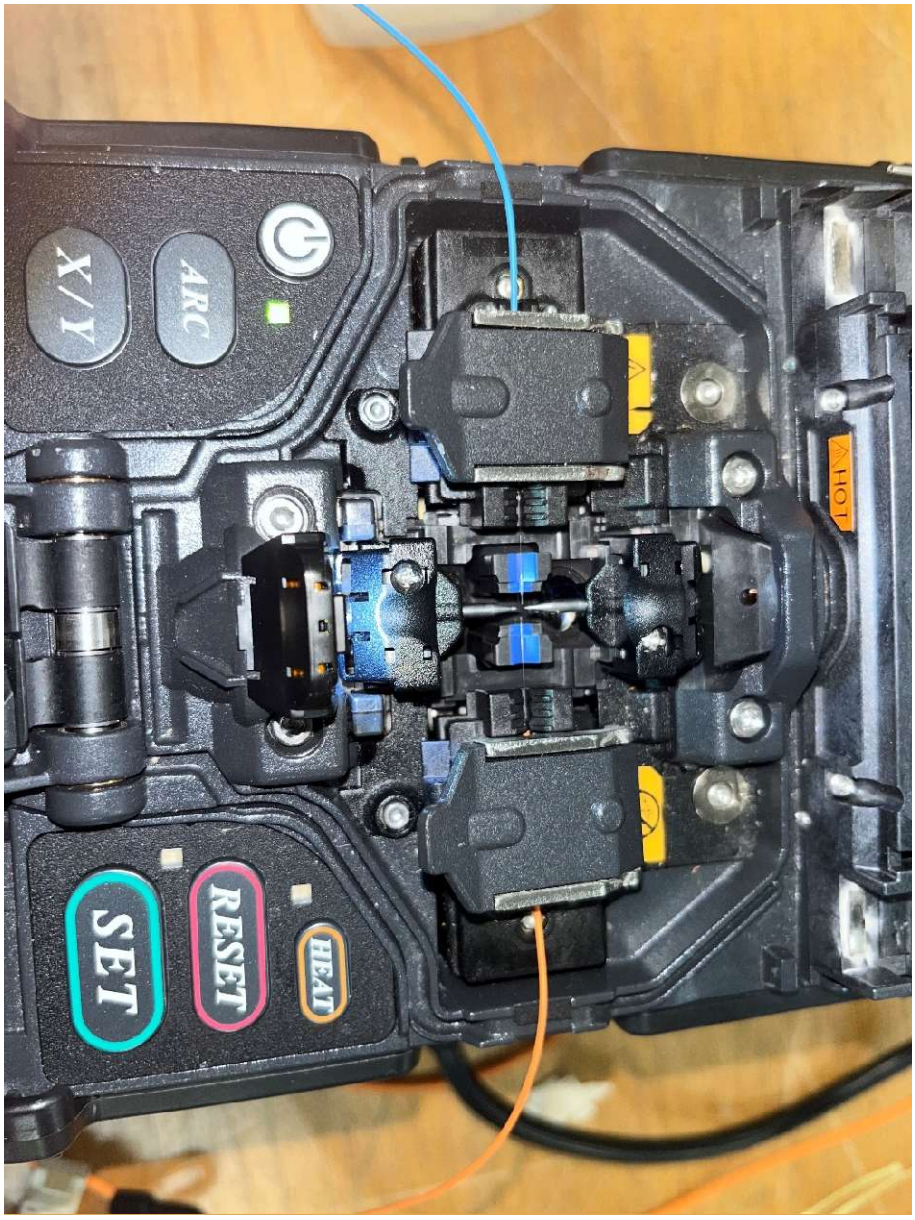


La deuxième étape consiste à enlever la gaine bleu pour pouvoir directement la fibre

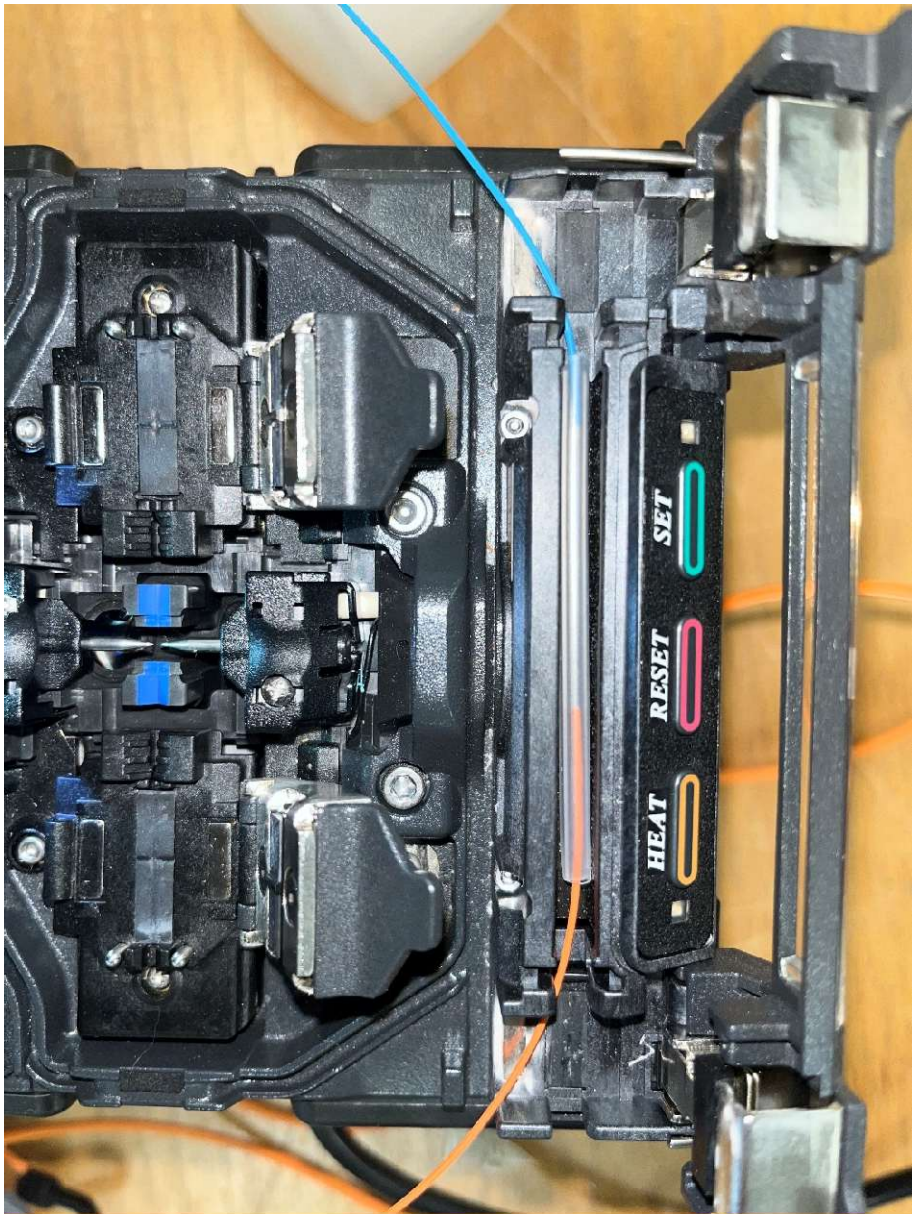

250
20
18
16
14
12
10
8

La troisième étape consiste à mettre la fibre dans un outil qui va permettre de couper proprement la fibre afin de pouvoir la soudé par la suite. Il faudra donc faire ça sur les deux fibres.

Après il faudra mettre le bout des deux fibres dans cet outil qui est la soudeuse.




La dernière étape consiste à mettre un bout de plastique et de le bruler grâce au même outil ce qui permet de protéger la fibre.




---

Conclusion

Ce stage m’a permis d’enrichir mes compétences techniques de manière concrète, en particulier dans les domaines réseau, système et sécurité. J’ai appris à m’adapter à un environnement exigeant, avec un haut niveau de confidentialité et une organisation rigoureuse. Ce fut une expérience très enrichissante tant sur le plan technique que personnel.