SACHA
MARQUES

MAI - JUIN 2024

RAPPORT DE STAGE 1ÈRE ANNÉE BTS

CAMPUS SAINT-ASPAIS MELUN

Sommaire

Introduction

During my first year of BTS SIO, I did an internship at FAST WINDOWS, a company specialising in cybersecurity and programming with a network component this company is a self-employed entrepreneur so there were only two of us and my internship supervisor working from home. The aim of this placement was to put into practice some of the points we'd covered during the course and to find out about a professional environment that was as close as possible to our sector of activity. With the particular context of teleworking, the placement was different from the others I'd already done during this placement, which I had the opportunity to attend. Despite everything, this placement was special because it involved teleworking, which is an important point in my analysis of this placement.

Plan :

Chapter 1 deals with the company (...)

Then, in Chapter 2, the subject will be a set of specifications with objectives for the course, accompanied by diagrams and images.

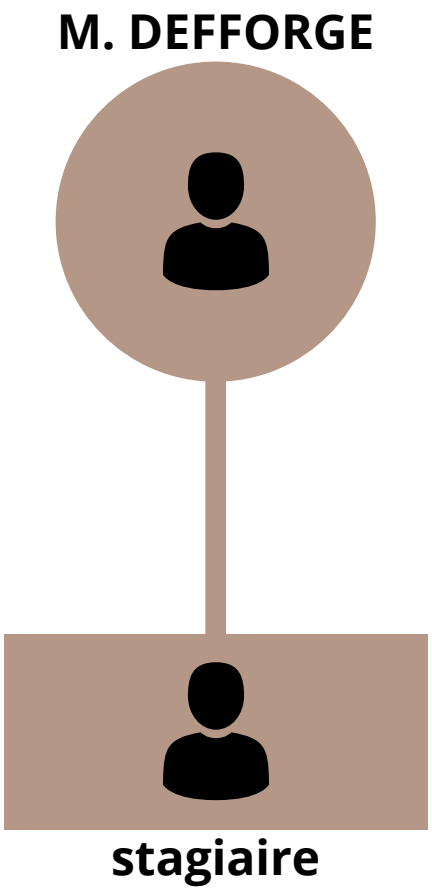
Chapter 3 will focus on the work carried out, with technical explanations and detailed information on the subject.

Then we'll finish with a conclusion and a summary.

Chapitre 1

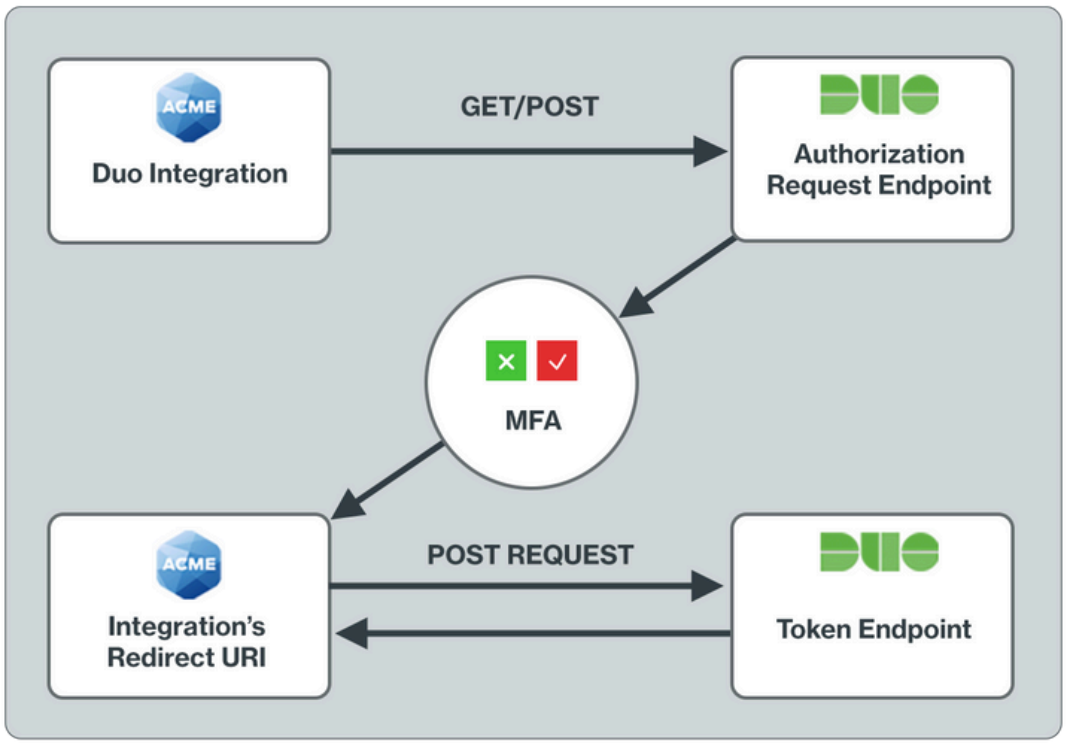
Tout d'abord l'entreprise qui m'a accueilli pour ce stage est FAST WINDOWS dans un contexte assez particulier (télétravail) qui devient de plus en plus courant. En effet FAST WINDOWS est une auto-entreprise qui ne possède pas de locaux à proprement parler mais fonctionne plutôt avec un concept répondant aux besoins des entreprises avec des outils de gestion à distance.
Mon maître de stage M. DEFFORGE était donc aussi le créateur et président de FAST WINDOWS. Comme indiqué précédemment M. DEFFORGE ne possède pas de locaux nous avons donc communiqué via l'application WhatsApp en respectant les heures indiquées sur la convention de stage ainsi que les pauses.

Dans le contexte de mon stage chez M. DEFFORGE je regrette de ne pas avoir eu l'occasion d'accéder à des machines distantes de tiers comme celles des clients de FAST WINDOWS.



Chapitre 2

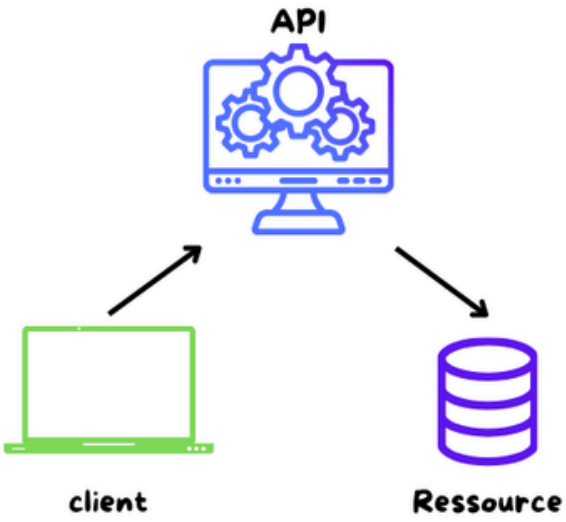
Les objectifs de ce stage étaient d'abord d'acquérir une première expérience professionnelle dans un stage en télétravail différent des stages que j'avais effectué pendant les années de lycée. Dans un contexte particulier comme celui du télétravail, surtout pour un étudiant de première année, les objectifs étaient bien différents de ceux d'un stagiaire dans un service en présentiel. En effet, les attentes de mon tuteur de stage étaient plus théoriques, et je devais appliquer avec lui et moi-même les solutions de sécurité que nous avons eu l'occasion de mettre en œuvre.
À multiples reprises mon tuteur m'a demandé de consulter la fiche pédagogique et d'analyser les documentations et les outils que nous utilisions pour les mettre en lien avec cette fiche et ainsi pouvoir compléter toutes les tâches nécessaires au bon déroulement de ce stage.
Nous avons commencé par l'utilisation de l'outil DUO Cisco et comment le mettre en place. Un exemple d'utilisation de DUO :



Avec l'utilisation de MFA (Authentification multifacteurs) nous avons donc eu l'occasion de sécuriser des applications avec une double authentification.
Mon tuteur attendait de moi une certaine rigueur et autonomie. Même si nous étions très souvent en contact, parfois il n'avait pas le temps de me répondre pendant quelques temps et il attendait donc une certaine autonomie que j'ai réussi à développer tout au long du stage. Cette autonomie m'a permis de m'améliorer et pourrait m'être utile dans les années d'études qu'il me reste.

Chapitre 2

Ensuite pour l'aspect technique, les premières semaines se sont concentrées sur la cybersécurité et la sécurisation des accès avec des API, notamment avec Cisco DUO pour l'authentification à deux facteurs. Nous avons ensuite utilisé des outils comme POSTMAN pour continuer sur l'utilisation des API. POSTMAN permet la création d'API et de comprendre leur utilisation en entreprise que ce soit les API REST ou les API SDN qui permettent de contrôler un réseau.



Mon tuteur m'a aussi incité à créer des fiches de procédures que je pourrais introduire plus tard dans mon portfolio à rendre en deuxième année (cf. annexe 1 pour ces procédures).

J'ai aussi eu l'occasion d'assister à des réunions en visioconférence avec mon maître de stage notamment avec l'entreprise DATADOG. En effet mon maître de stage qui est aussi le patron de l'entreprise souhaitait collaborer avec cette entreprise pour mettre en place une structure potentielle avec les outils de Datadog pour visualiser et créer des alertes sur des serveurs cloud notamment AWS utilisés par M. Defforge.

Chapitre 3

Tout d'abord les journées se présentaient de la façon suivante : je me levais avant le début de mon stage pour allumer mon ordinateur et préparer mes appareils. Puis je me rendais sur WhatsApp pour me connecter et communiquer avec mon maître de stage. Le télétravail est particulier car cela demande beaucoup de concentration et un environnement stable avec des appareils adaptés. J'ai pu effectuer mon stage dans de bonnes conditions grâce à un ordinateur fixe avec une bonne capacité de RAM (utile pour les tâches que j'ai effectué) et un portable en cas de besoin.

Je vais d'abord vous parler des soucis que j'ai rencontré dans cette configuration exceptionnelle de stage en télétravail. En effet je possède chez moi une fibre haut débit qui m'a permis de rester connecté en toute circonstance tant que j'étais chez moi. Mais malheureusement des soucis se sont posés, en effet les coupures de courant ou d'internet pour régler les soucis se font souvent en journée pour ne pas déranger les particuliers qui sont pour la plupart au travail. Mais pour ceux en télétravail cela pose problème. J'ai donc dû faire face à plusieurs soucis techniques comme une coupure de courant qui a duré toute l'après-midi, heureusement j'avais été prévoyant en gardant un ordinateur toujours chargé et de la 4G à ma disposition. Ensuite une coupure internet a eu lieu un autre jour pour une durée indéterminée ce qui m'a poussé à appeler le service de mon FAI afin de recevoir des recharges 4G en expliquant que j'étais en télétravail. Heureusement la couverture 4G de ma ville est de très bonne qualité.

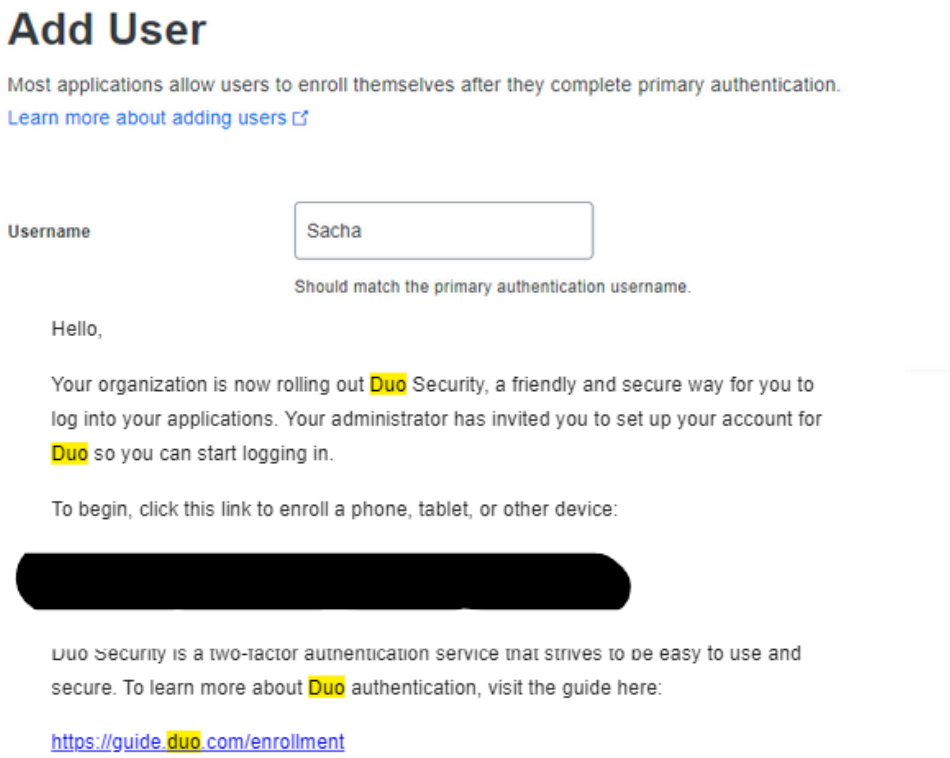
Maintenant que le cadre de ma situation de stage est posé je vais vous présenter les tâches que j'ai pu effectuer en stage en choisissant celles qui m'ont été bénéfiques. Tout d'abord la première tâche était l'utilisation de l'outil DUO de Cisco qui offre une solution de gestion et d'administration des accès aux ressources du SI d'une entreprise. Cisco DUO est un outil très complet qui offre une polyvalence très intéressante j'ai donc commencé par créer un compte avec l'entreprise de M. DEFFORGE puis j'ai commencé à explorer et comprendre comment fonctionne cet outil, comme je l'ai appris avec les cours de BTS SIO j'ai recherché de la documentation officielle, j'ai lu analysé et récupéré ce qui était important pour mon utilisation.

En cours de cybersécurité notre professeure insiste souvent sur les trois bases de la cybersécurité (Confidentialité Intégrité Disponibilité) et grâce à cet outil j'ai réussi à répondre à tous ces critères. Pour m'expliquer je vais vous détailler l'utilisation de CISCO DUO et je vais vous présenter une tâche en lien avec ceci.

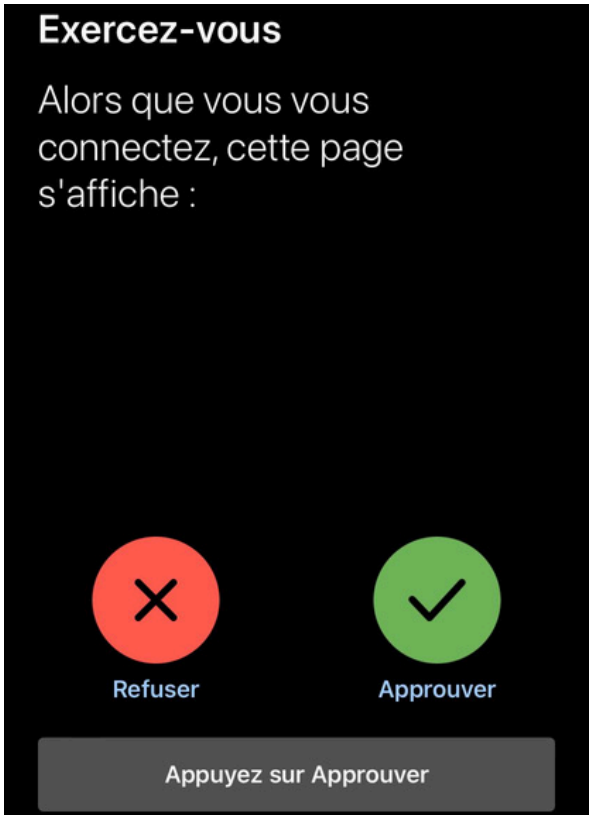
Pour continuer Cisco DUO est un site qui propose aux entreprises peu importe leur taille, ainsi qu'aux particuliers avec de l'expérience de mettre en place une solution MFA centralisée qui utilise des protocoles de sécurité puissants. Avec DUO CISCO et un abonnement à leur service, un administrateur peut sécuriser les accès aux applications utilisées dans son SI ainsi qu'aux machines tout en simplifiant l'expérience des utilisateurs. J'ai donc simulé cela en mettant en place une A2F connectée avec un service pour vous montrer cet outil et pour cela j'ai choisi un autre outil très utile en cybersécurité : LastPass qui crée une banque de mot de passe et chiffre les mots de passe.

Chapitre 3

Avant de vous montrer comment j'ai sécurisé LastPass il faut d'abord créer un compte utilisateur pour lui donner accès à certaines ressources et en bloquer d'autres. Pour cela, il suffit d'ajouter l'utilisateur à DUO avec son prénom et son nom. Il sera ensuite invité par un lien à ajouter son numéro de téléphone et son e-mail (en cas de perte de moyen d'accès à ses ressources l'administrateur peut modifier ces informations). Pour cela je me suis référé aux manuels DUO Cisco en annexe.

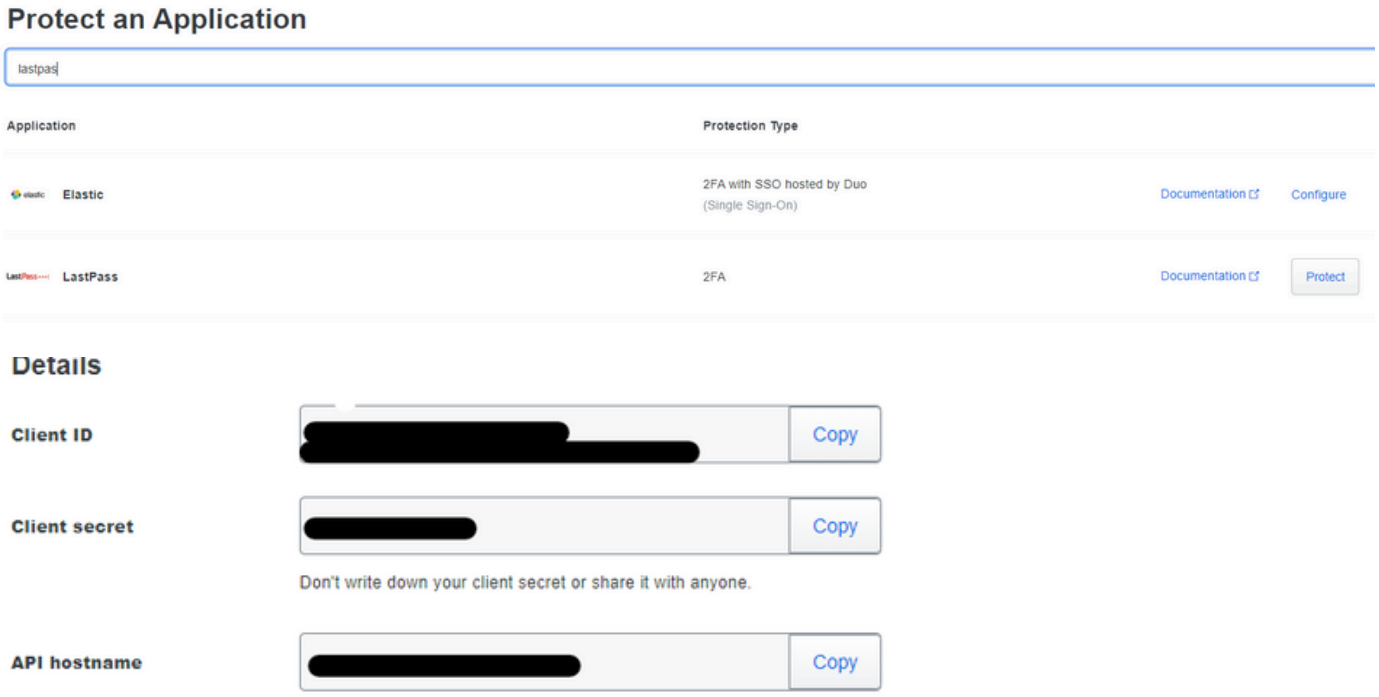


Une fois ajouté il faut faire installer l'application DUO à l'utilisateur sur son téléphone. Pour simplifier il sera invité à scanner un QR code sur l'application pour l'aider à comprendre son fonctionnement. Une fois prêt, il sera invité à approuver ou refuser des connexions. Voici des exemples pour comprendre le fonctionnement de l'outil :



Chapitre 3

Une fois les utilisateurs ajoutés, nous pouvons maintenant sécuriser une application comme LastPass. J'ai donc commencé par créer un compte sur LastPass, puis j'ai configuré la sécurisation avec DUO en ajoutant LastPass comme ceci :



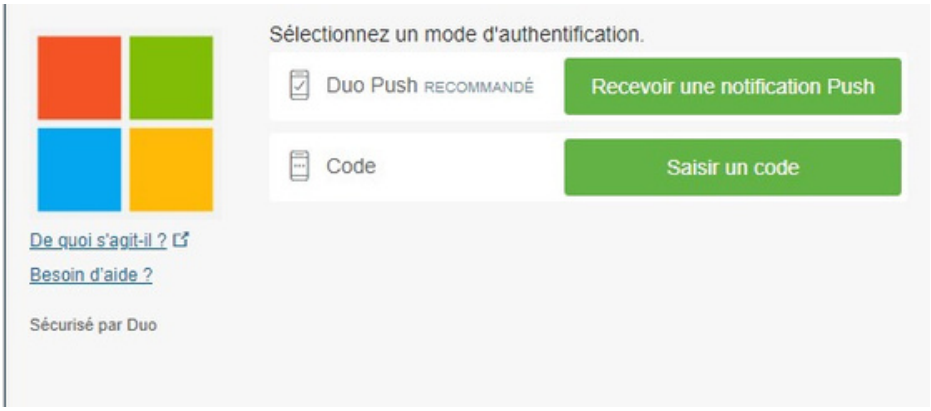
Ensuite, j'ai reçu un CLIENT ID, un CLIENT secret et une API qui vont me servir à sécuriser mon application. L'API permet à LastPass de communiquer avec Cisco DUO pour sécuriser l'accès, si l'utilisateur n'a pas d'accès il sera bloqué du service.

Option	Valeur
Activé	Oui
Autoriser l'accès hors ligne	Autoriser
Utiliser le SDK Duo Web si possible	Oui
Clé d'intégration	
Clé secrète	
Nom d'hôte d'API	
En savoir plus	Manuel d'aide

Pour finir j'ai ajouté mes informations à LastPass.

Chapitre 3

Mon application est maintenant sécurisée. À chaque connexion, cette page va s'afficher :



L'utilisateur va donc choisir si il veut une notification ou un code aléatoire utilisable qu'une fois qui se génère sur l'application.

L'utilisateur sera alors invité à se connecter à DUO pour s'assurer qu'il possède bien les droits d'accéder à l'application. Avec DUO nous pouvons donc répondre à l'authentification forte qui repose sur : ce que je sais, ce que je possède, ce que je suis.

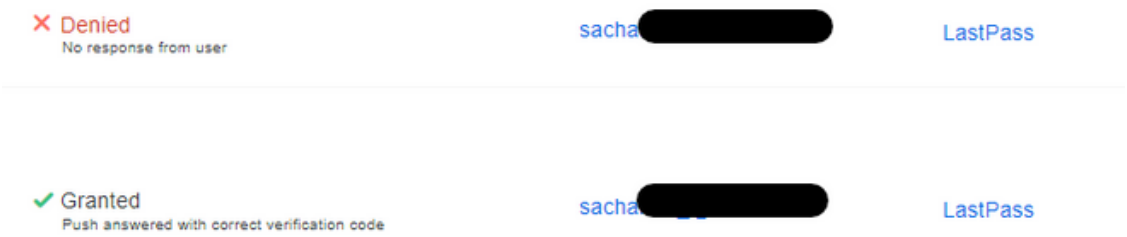
ce que je possède
(l'application DUO, clé de secours)

ce que je sais
(mot de passe DUO)

ce que je suis
(connexion avec les données FACE ID à DUO)

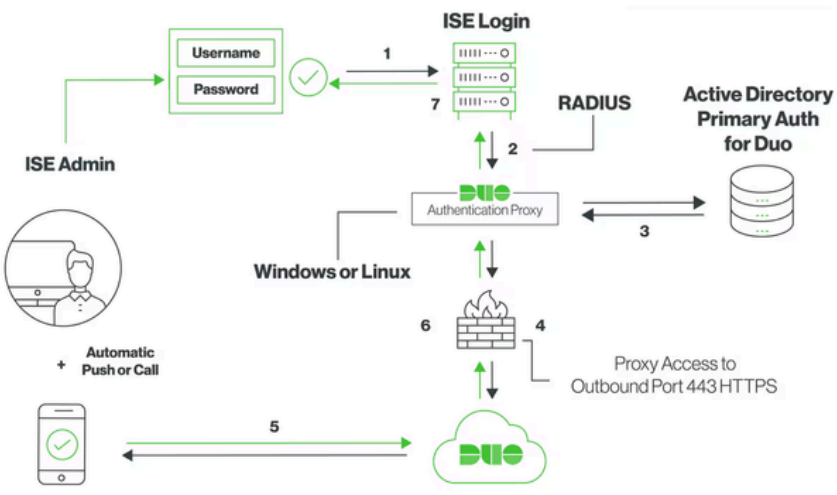
Chapitre 3

En continuant avec DUO Cisco, qui possède une interface d'administration complète, il est possible de voir en temps réel quels utilisateurs se connectent et ceux qui sont bloqués par DUO en cas d'impossibilité de prouver leur identité.



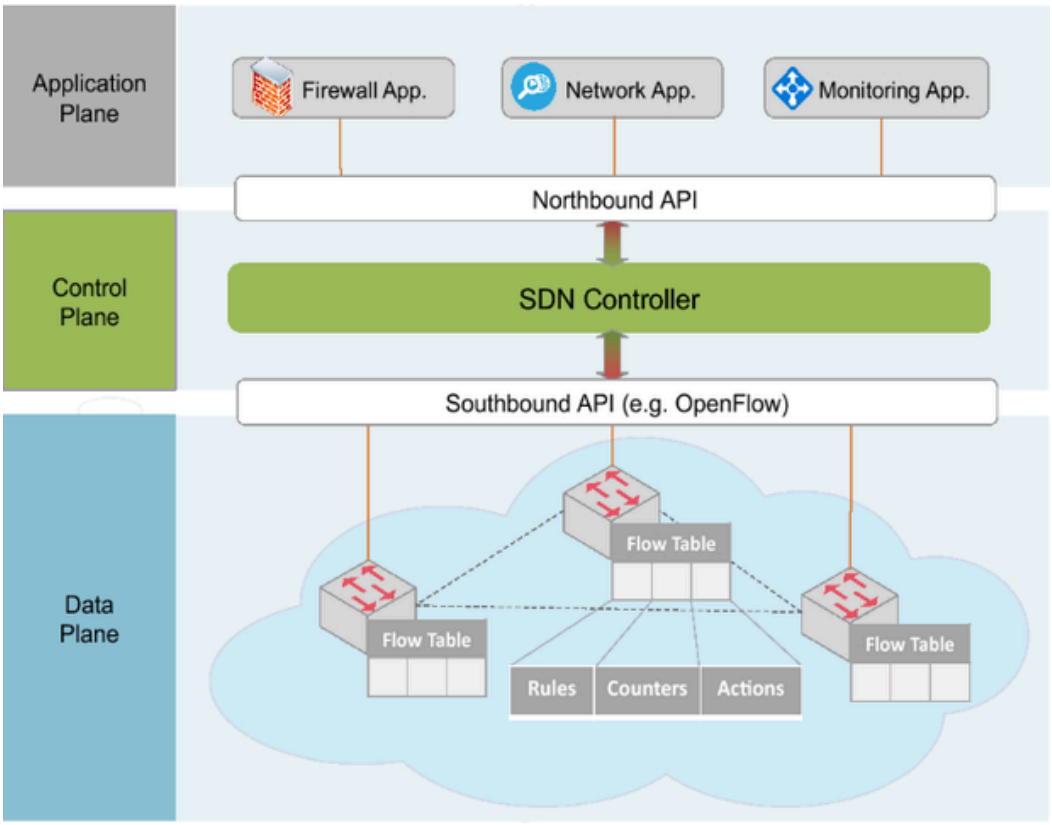
Il est également possible d'appliquer des règles de filtrage pour les utilisateurs qui tentent de s'inscrire aux services, avec des règles telles que :

Ces règles pourraient servir à bloquer certaines versions d'OS de téléphone qui pourraient contenir des failles notables capables de mettre en danger le SI. Nous pouvons aussi bloquer par exemple des navigateurs ou autres qui pourraient représenter un danger dans une entreprise. Pour une utilisation plus poussée, nous pouvons par exemple installer DUO sur une machine à l'aide de RDP et donc configurer une authentification à deux facteurs sur un ordinateur. Pour conclure sur DUO Cisco c'est un outil très complet qui permet de mettre en place un système de sécurité robuste en authentification à deux facteurs, facile à utiliser pour les utilisateurs et très complet pour les administrateurs.



Chapitre 3

Ensuite, nous avons eu l'occasion d'explorer et d'utiliser l'outil POSTMAN qui permet la gestion des API ainsi que l'utilisation d'API existantes. Tout d'abord, les APIs (Interfaces de Programmation Applicative) sont des "programmes" qui facilitent l'échange de données et d'informations. L'objectif était donc de comprendre l'utilisation des APIs pour potentiellement l'appliquer avec une API SDN (Software-defined networking).



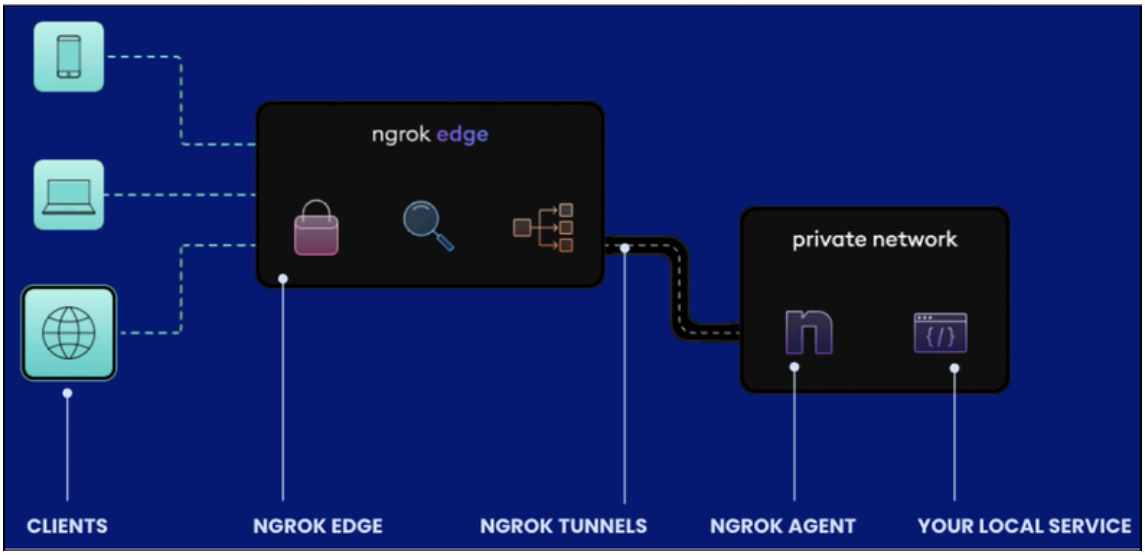
Grâce à ces APIs, il est possible de gérer des VLAN, des ACL, et d'automatiser certaines tâches. Malheureusement, le manque de structures de l'entreprise ne m'a pas permis de gérer un contrôleur SDN et d'automatiser ou modifier des tâches avec des APIs. Néanmoins, j'ai travaillé à la compréhension de cet outil complexe qui m'était inconnu auparavant et qui est largement utilisé en entreprise.

Malgré tout, avec mes recherches j'ai trouvé un document de l'ANSSI qui explique que le fait de "centraliser" sur un seul serveur la gestion de toute la structure réseau pouvait poser un problème et que des sécurités fortes étaient à prévoir, notamment l'utilisation de SSL / TLS et l'utilisation de système de détection d'intrusion.

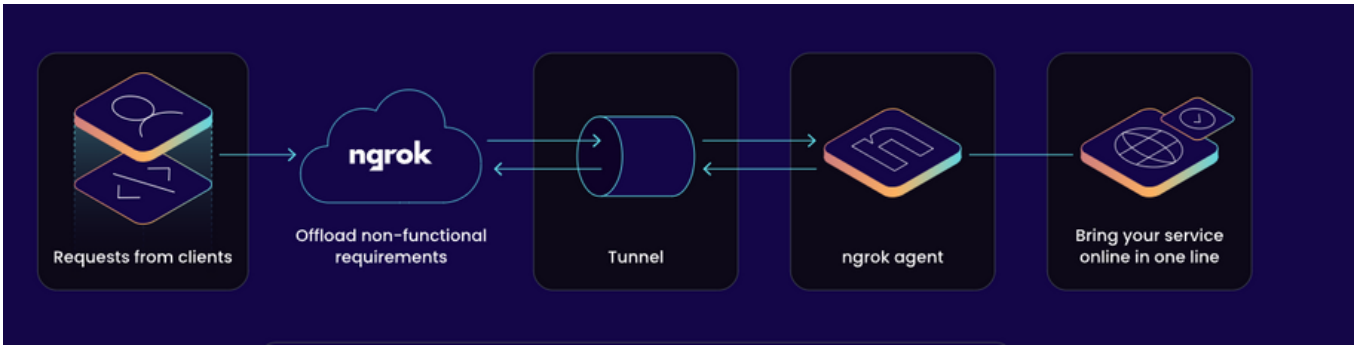
Chapitre 3

Pendant ce stage, j'ai aussi eu l'occasion d'utiliser l'outil NGROK avec M. DEFFORGE et de consulter les documentations pour comprendre comment fonctionnait cet outil.

NGROK est un outil qui permet de partager un site web local sans l'héberger sur un serveur web et donc permettre le test ou la collaboration entre les employés qui travaillent sur un projet commun.



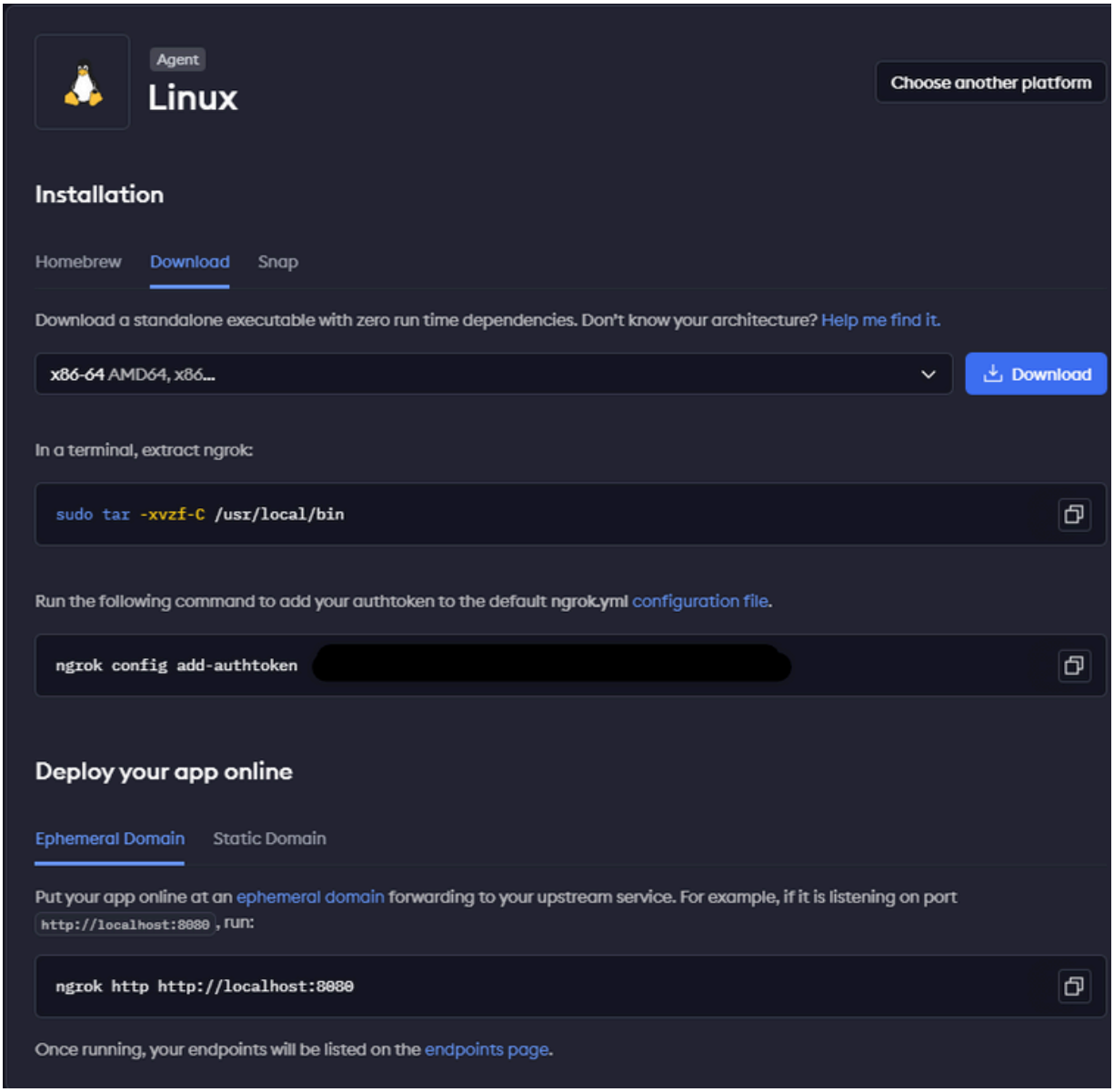
NGROK permet donc à des développeurs de collaborer ou de tester des API en créant un tunnel sécurisé qui va permettre la collaboration.



NGROK est donc une solution très intéressante, surtout pour les petites entreprises comme FAST WINDOWS, puisqu'il s'agit d'une solution gratuite et fonctionnelle pour tester des API et des sites sans avoir à prendre un abonnement chez un hébergeur. Elle possède aussi un avantage majeur, lors de la création d'un tunnel aucun port ne nécessite d'être ouvert et l'accès se fait avec un lien généré automatiquement avec un algorithme complexe qui augmente la sécurité de l'outil.

Chapitre 3

NGROK s'installe donc sur la machine où le serveur local est hébergé (Apache...) puis il faut installer et tester le site via NGROK en installant NGROK sur la machine et en testant comme ceci :



On ajoute ensuite le token d'accès à NGROK :

```
sacha@sacha-VirtualBox:~/Bureau$ ngrok config add-authtoken [redacted]
```

Puis on ouvre le tunnel.

```
sacha@sacha-VirtualBox:~/Bureau$ ngrok http http://localhost:8080
```

Conclusion

En conclusion, pendant ce stage, j'ai dû m'adapter aux conditions de l'entreprise en apprenant à télétravailler avec des outils comme WhatsApp et Zoom. Les tâches que j'ai effectué étaient plus de l'ordre du théorique que du véritable contact avec des clients. J'ai eu l'occasion de préparer et simuler l'infrastructure de M. DEFFORGE.

Lors de ce stage, mon maître de stage a aussi beaucoup insisté sur l'analyse et la compréhension des tâches que nous effectuons et des documents qui m'étaient transmis.

Nous avons aussi eu l'occasion d'optimiser la communication de FAST WINDOWS, notamment avec le compte GitHub de M. DEFFORGE ainsi que les réseaux sociaux.

J'ai aussi eu la chance de participer à une réunion ZOOM avec l'entreprise DATADOG qui fournit des statistiques et crée des alertes pour les serveurs cloud.

J'ai aussi eu l'occasion de participer activement au développement de l'entreprise en participant aux réunions de stratégies avec des outils comme AWS et des serveurs cloud.

Nous avons donc réussi à améliorer la performance de l'entreprise et peut-être réussir à ramener d'autres clients qui voudraient gérer des serveurs ou qui cherchent un site à créer.

J'ai aussi eu la chance de développer de nouvelles compétences, d'être plus à l'aise avec l'utilisation de mon ordinateur. J'ai dû apprendre à bien classer mes documents et conserver les ressources qui m'étaient données à des endroits où je pourrais les retrouver.

Avec toutes les ressources des entreprises que nous avons utilisé, les outils, j'ai sûrement pris de l'avance sur le programme de l'année prochaine. J'ai aussi développé ma connaissance des outils qui existent et de comment je pourrais les appliquer plus tard dans mon métier à la fin de mes études (notamment avec DUO Cisco). J'ai aussi réfléchi aux futures carrières qui pourraient s'ouvrir à moi, notamment en étudiant le parcours de M. DEFFORGE, qui a su développer et créer une entreprise.

Dans un monde en mouvement numérique constant, M. DEFFORGE m'a aussi incité à continuer les veilles technologiques et développer mon réseau pour me renseigner et ainsi utiliser des listes comme le top 10 OWASP. Nous avons aussi trouvé une veille technologique commune puisque la mienne porte sur le GREEN IT et qu'il est président d'une association dans le domaine du GREEN IT, ce qui m'a permis de renforcer mon engagement dans ma veille technologique.

Conclusion

Pour finir, je vais vous parler de mon expérience professionnelle et humaine pendant ce stage de 6 semaines. Tout d'abord, lors de nos études, le télétravail en informatique est un sujet omniprésent. En effet, le secteur de l'IT fait parti des secteurs qui comptent le plus d'employés en télétravail, qu'ils soient partiellement ou à 100 %.

De ce fait, j'envisageais clairement de télétravailler si cela était possible à la fin de mes études. Cependant, mon regard sur le télétravail a bien changé après ce stage. Certes, télétravailler offre plus de temps pour les activités personnelles (le temps de transport étant déduit), mais le fait de travailler et d'effectuer des tâches dans le réseau qui est un secteur qui demande beaucoup de contact humain et de présence physique m'a fait prendre conscience que les métiers que nous pouvons faire après nos études ne sont pas totalement adaptés au télétravail. Gérer un utilisateur mécontent ou gérer un serveur à distance n'est pas optimal, et le télétravail serait peut-être plus adapté à de la programmation qu'à du réseau.

Personnellement cette expérience m'a permis de prendre conscience que pour un travail à plein temps je ne me retrouve pas dans le télétravail. Même si j'ai réussi à garder une rigueur et à rester actif pendant le stage, le rythme était parfois difficile à suivre et les contacts humains étaient manquants surtout pour recevoir de l'aide ou comprendre des problèmes dans nos activités. De plus, la télécommunication peut parfois mener à des incompréhensions et causer plus de problèmes qu'initialement.

Pour finir sur cette conclusion, le stage m'a été très bénéfique. J'ai vu une face du monde professionnel qui est de plus en plus courante (le télétravail).

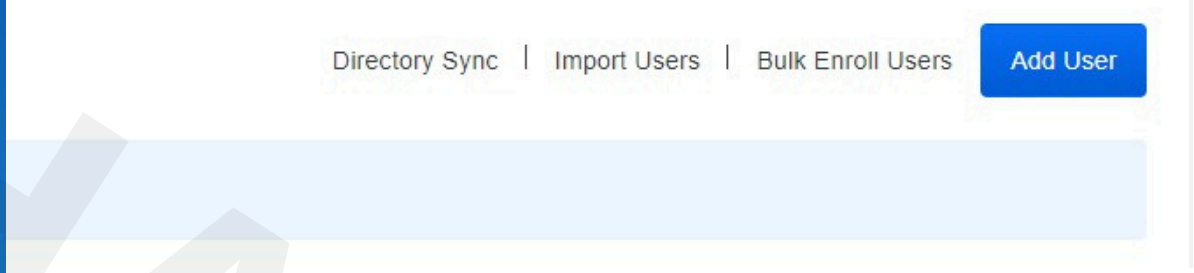
Malgré tout, j'ai beaucoup appris surtout sur ma capacité à être autonome et à rechercher des informations fiables et de bonne qualité sans avoir à demander tout le temps de l'aide, même si souvent l'aide d'une personne expérimentée reste très importante. Je pense donc être sorti grandi de ce stage, d'avoir appris beaucoup et de maintenant être en capacité d'appliquer toutes ces connaissances dans le monde professionnel et de pouvoir aussi les appliquer pendant les heures de cours qu'il me reste pour finaliser mes études.

J’aimerais finir en remerciant M. DEFFORGE de m’avoir accueilli et des mes professeurs d’être restés en contact avec moi pour prendre de mes nouvelles.

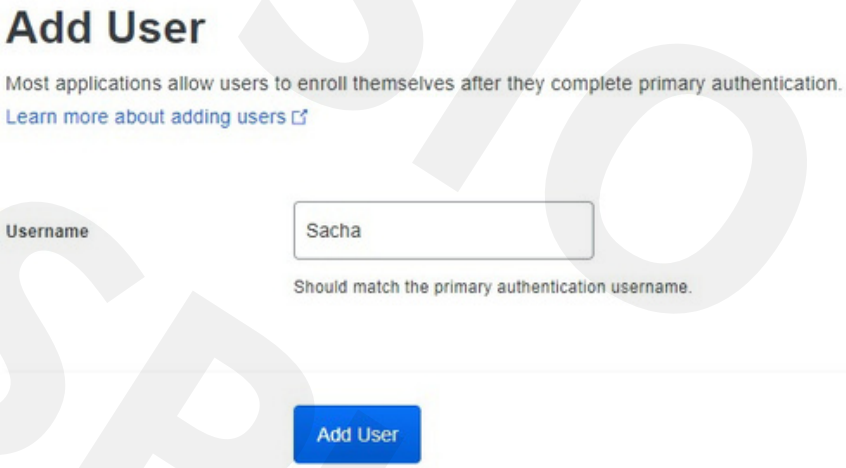
ANNEXES

PROCEDURE 1 DUO

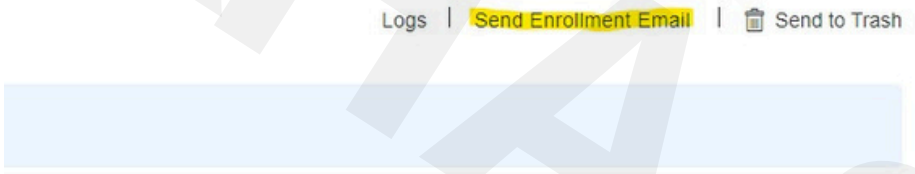
Cliquez sur ADD USER



Entrez le Nom choisi



Cliquez sur Send Enrollement Email



Ajout utilisateurs DUO cisco

L’utilisateur va recevoir un e-mail avec un lien

This is an automated email from Duo Security.

Your organization invites you to set up a user account for Duo. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

Hello,

Your organization is now rolling out Duo Security, a friendly and secure way for you to log into your applications. Your administrator has invited you to set up your account for Duo so you can start logging in.

To begin, click this link to enroll a phone, tablet, or other device:

[redacted]

Duo Security is a two-factor authentication service that strives to be easy to use and secure. To learn more about Duo authentication, visit the guide here:

https://guide.duo.com/enrollment

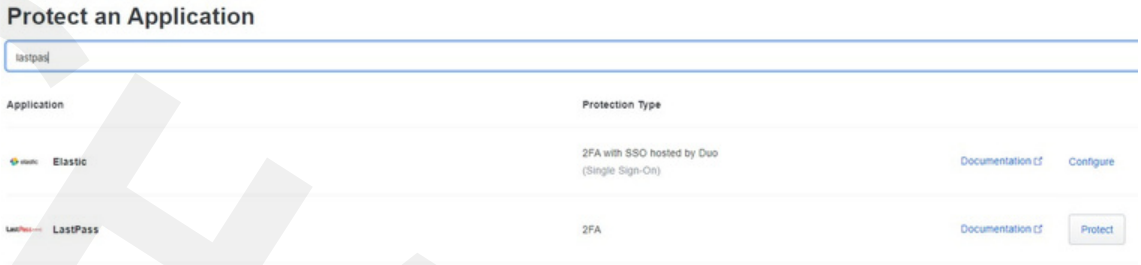
Puis il devra ajouter en suivant les instructions via numéro ou en scannant le QR code sur l’application DUO

Ajout utilisateurs DUO cisco

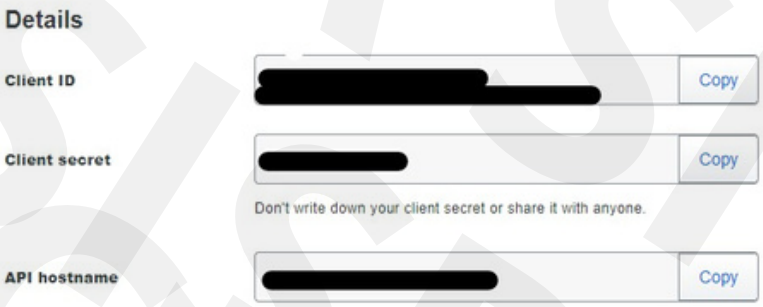
Il va ensuite recevoir une explication de l’utilisation automatique

PROCEDURE 2 DUO

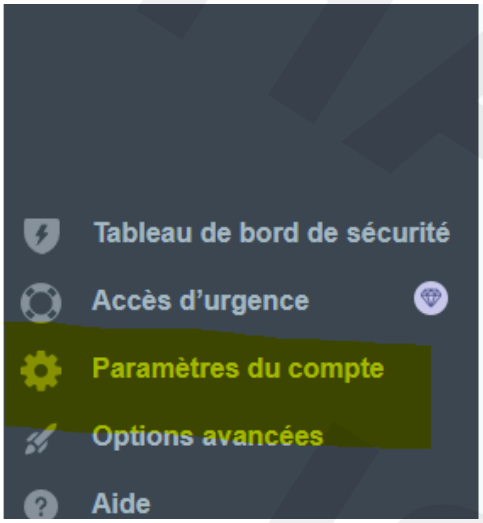
ajouter une application à protéger



Ensuite nous arrivons sur un menu dédié avec des informations



Maintenant rendons nous sur LAST PASS



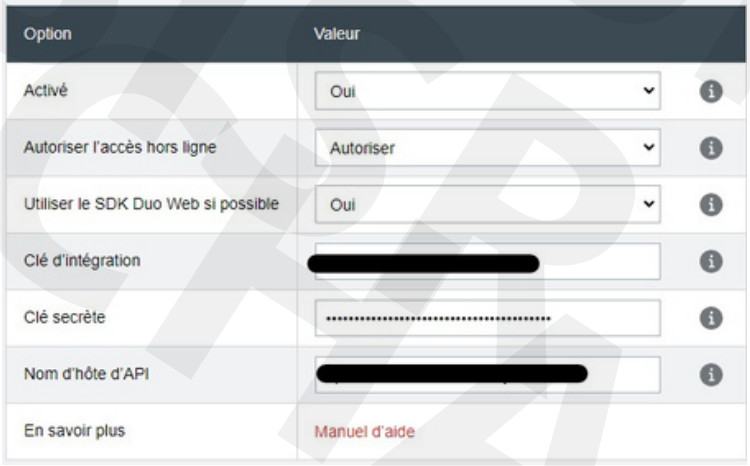
Puis paramètres de compte

Ajout utilisateurs DUO cisco

Options authentification multifacteur

On modifie :

On entre les informations vu précédemment sur duo :

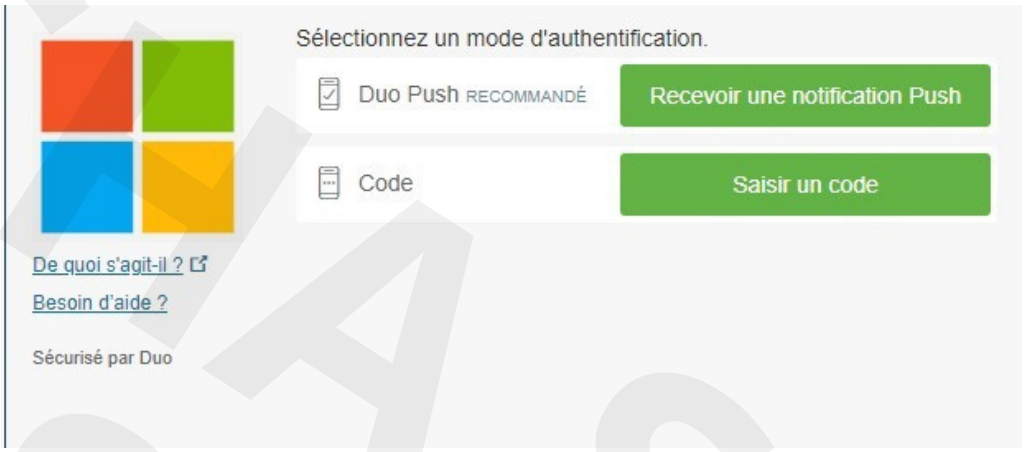


Puis mettre à jour :

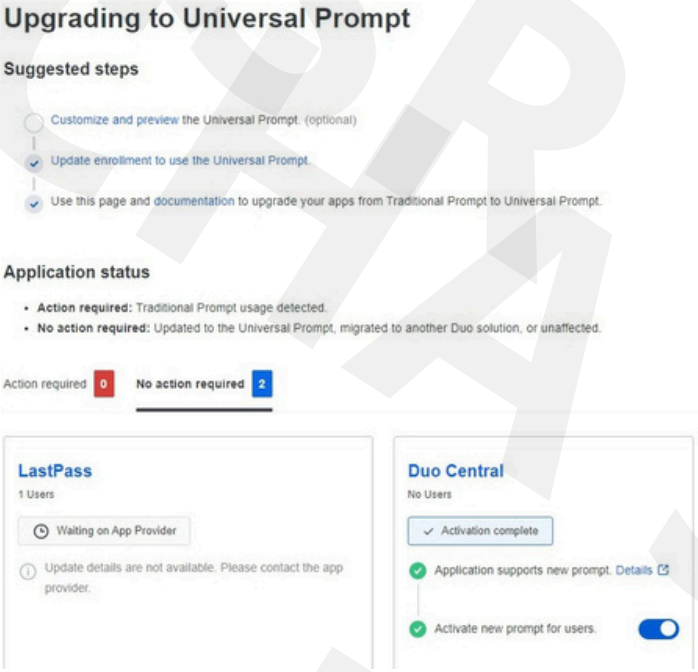
Ensuite un QR code va se présenter il faudra le scanner avec l'application pour lier les deux

Ajout utilisateurs DUO cisco

Ensuite à chaque connexion nous allons recevoir ceci :



Malgré tout il existe un moyen de sécurisé d'une meilleure façon les connexions pour cela allons activer le universal prompt



Une fois activé les connexions se feront par code comme ceci :

Ajout utilisateurs DUO cisco