

## **Nom de l'établissement :**

CFA ROBERT SCHUMAN

## **Réalisé par:**

AOURDOU BEN KHAYI BRAHIM

## **Date :**

08/01/2025

## **Encadrant :**

M.JACQUEMIN

## **Intro :**

Un pare-feu est un outil de sécurité informatique qui protège un réseau en contrôlant les connexions entrantes et sortantes. Il fonctionne comme un filtre qui décide si le trafic est autorisé ou bloqué en fonction de règles définies.

1: Un pare-feu est un dispositif de sécurité qui contrôle les connexions entre un réseau interne et l'extérieur, comme Internet. Il bloque ou autorise les échanges de données selon des règles prédéfinies, protégeant ainsi le réseau des attaques externes. Son rôle est d'empêcher les intrusions et de sécuriser les systèmes contre les menaces.

2: Pare-feu Matériels et pare-feu logiciel

3: Les pare-feu matériels offrent de meilleures performances et protègent l'ensemble du réseau, mais sont plus chers et difficiles à installer. Les pare-feu logiciels sont moins coûteux et plus flexibles, mais peuvent ralentir les systèmes et sont plus vulnérables.

4: - Filtrage des connexions réseau\*\* : Il bloque ou autorise les connexions en fonction des règles définies, comme les ports ou les adresses IP.

-Protection contre les intrusions\*\* : Il empêche les accès non autorisés à l'ordinateur ou au réseau.

-Journalisation des événements\*\* : Il enregistre les activités réseau pour détecter des actions suspectes et faciliter les analyses de sécurité.

-Contrôle des applications\*\* : Il permet de gérer quelles applications peuvent se connecter à Internet ou au réseau.

5: Panneau de configuration

-->Pare-feu Windows-Defender

--> Activer ou désactiver le pare-feu windows defender

6:

-Réseaux avec domaine : Réseaux en entreprise, qui appartiennent à un domaine

-Réseaux privés : Réseaux domestiques avec des appareils de confiance

-Réseaux Public : Réseaux dans les lieux publics tel que les aéroports, gare, ...

7: Ma machine se trouve dans un réseau avec domaine car je suis à l'école et que j'appartient au domaine SIO METZ.

8 : Une règle de pare-feu est une instruction qui détermine comment le pare-feu doit gérer le trafic réseau.

Elle définit des critères comme l'adresse IP, le port ou le protocole, et indique si le trafic doit être autorisé, bloqué ou redirigé, afin de protéger le réseau contre les connexions non souhaitées.

Pour en créer une sur le pare-feu Windows defender :

Panneau de configuration

-->Pare-feu Windows Defender

--> Paramètres avancés

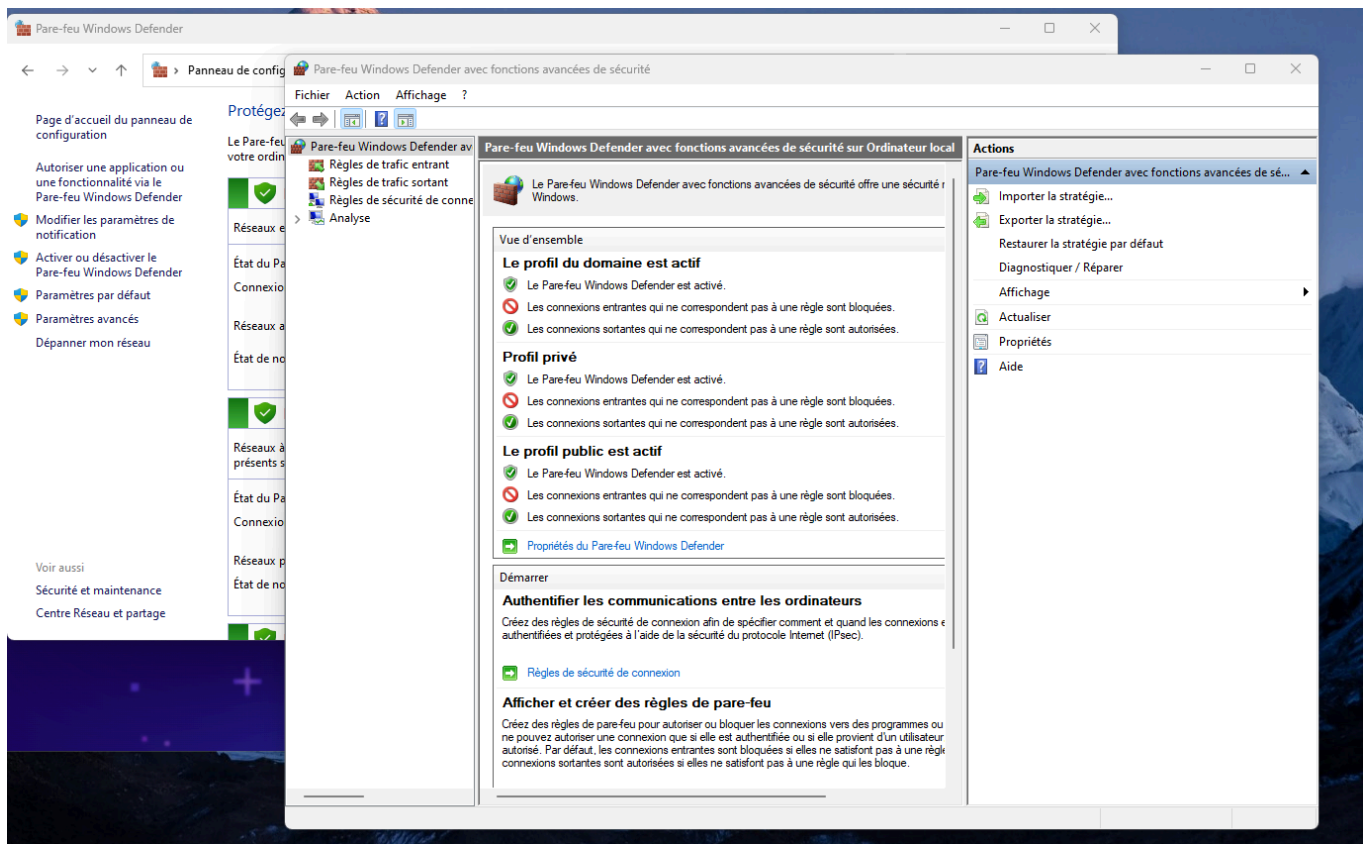
9:

-Règle entrante : elle contrôle le trafic entrant vers le pc ou le réseau ( autorise, bloque ou redirige l'entrée dans le réseau )

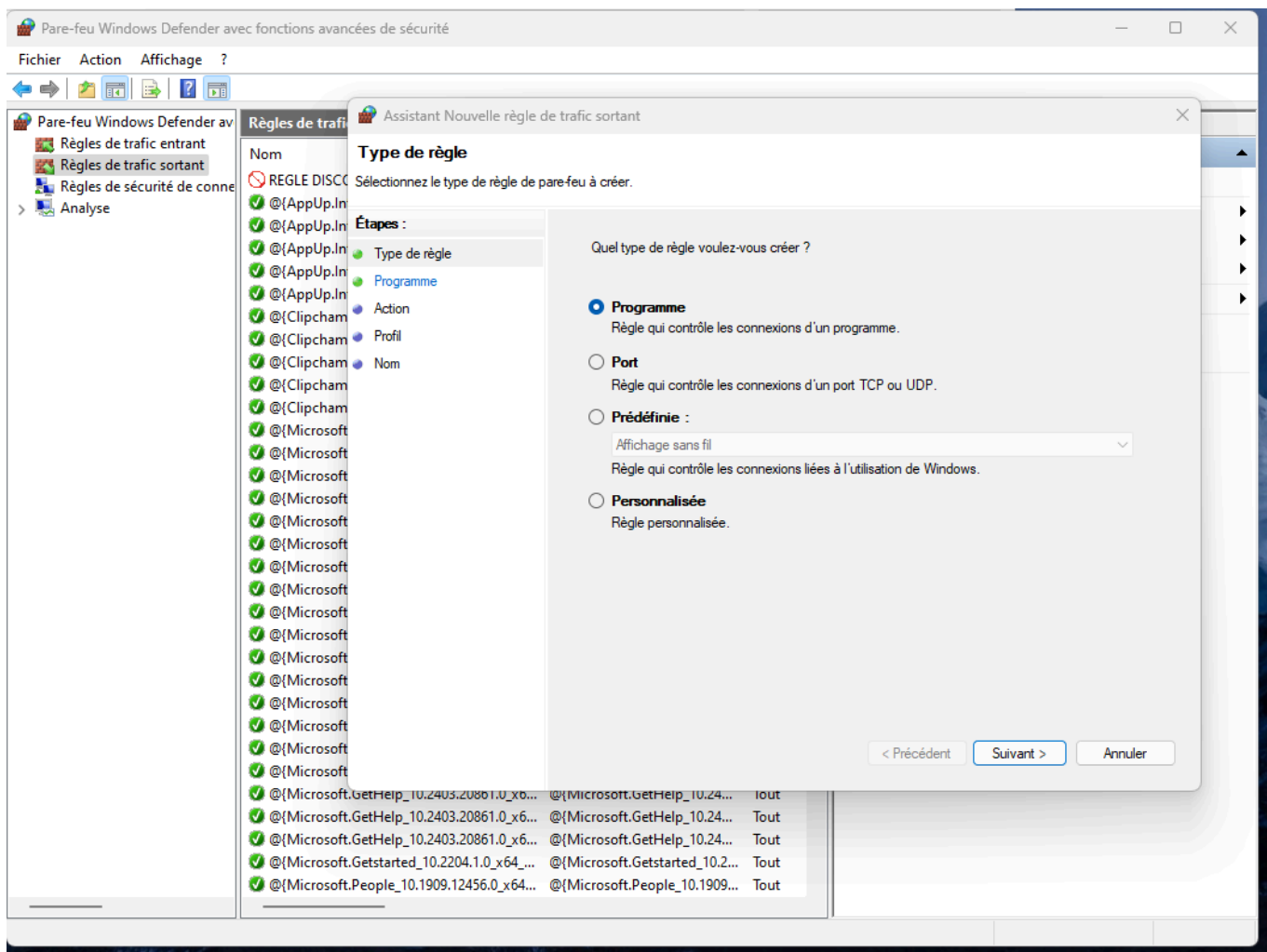
-Règle sortante : elle contrôle le trafic sortant du pc ou réseau vers internet(Détermine qui à le droit de sortir du réseau : bloque ou autorise l'accès à certains sites par exemple. )

10:

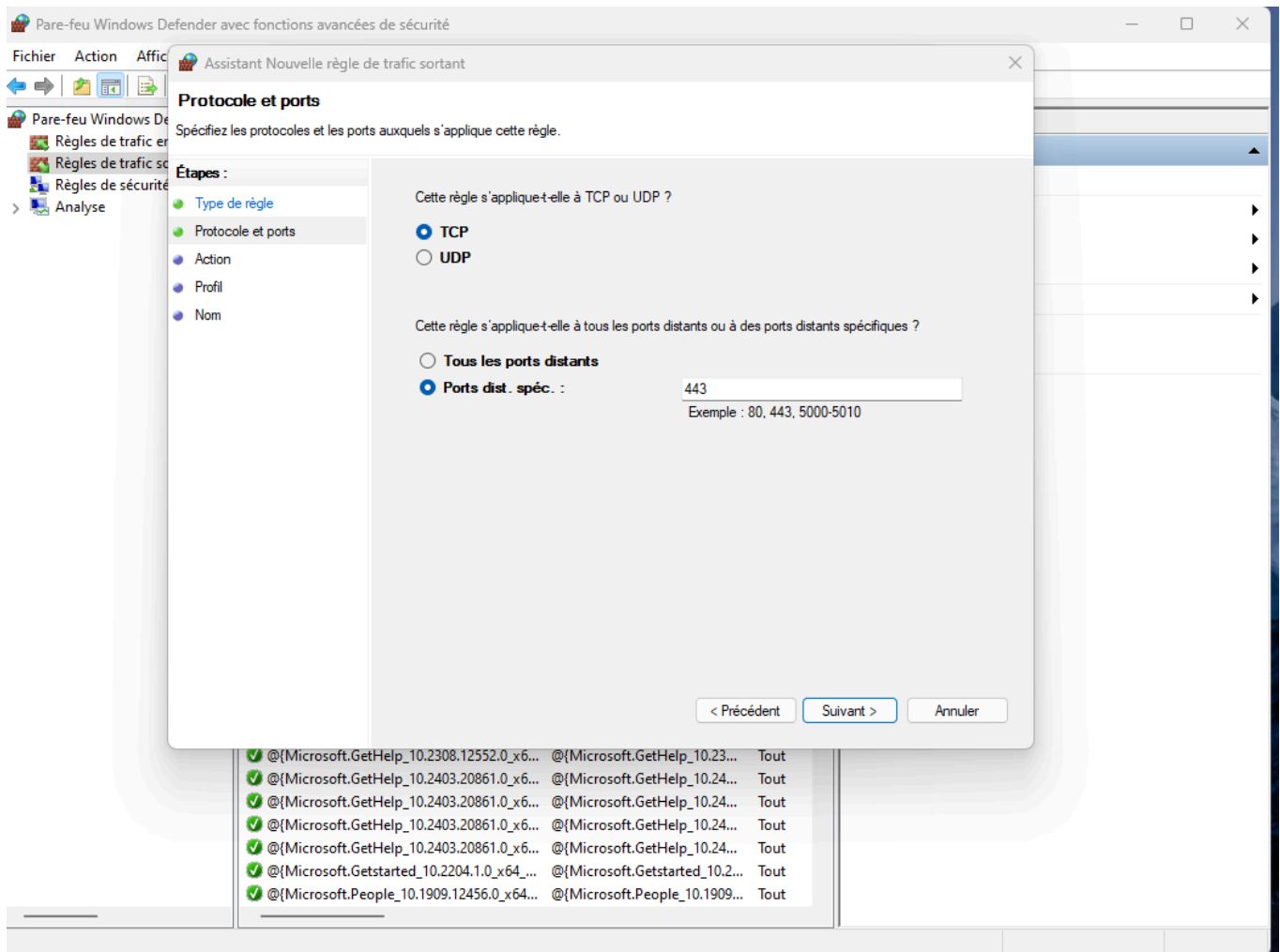
Bloques l'accès à discord avec le pare-feu Windows defender



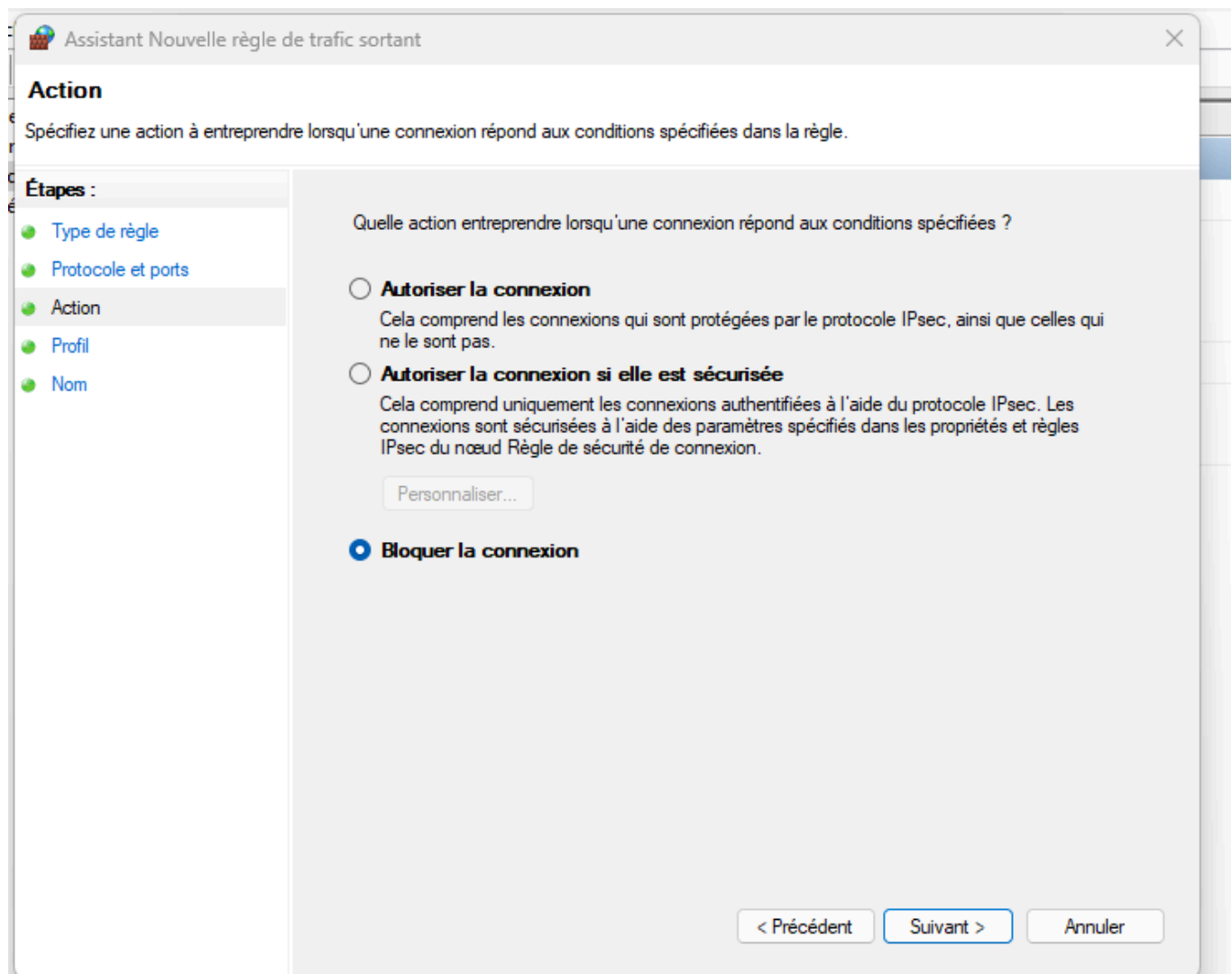
--> Nouvelle règle Sortante



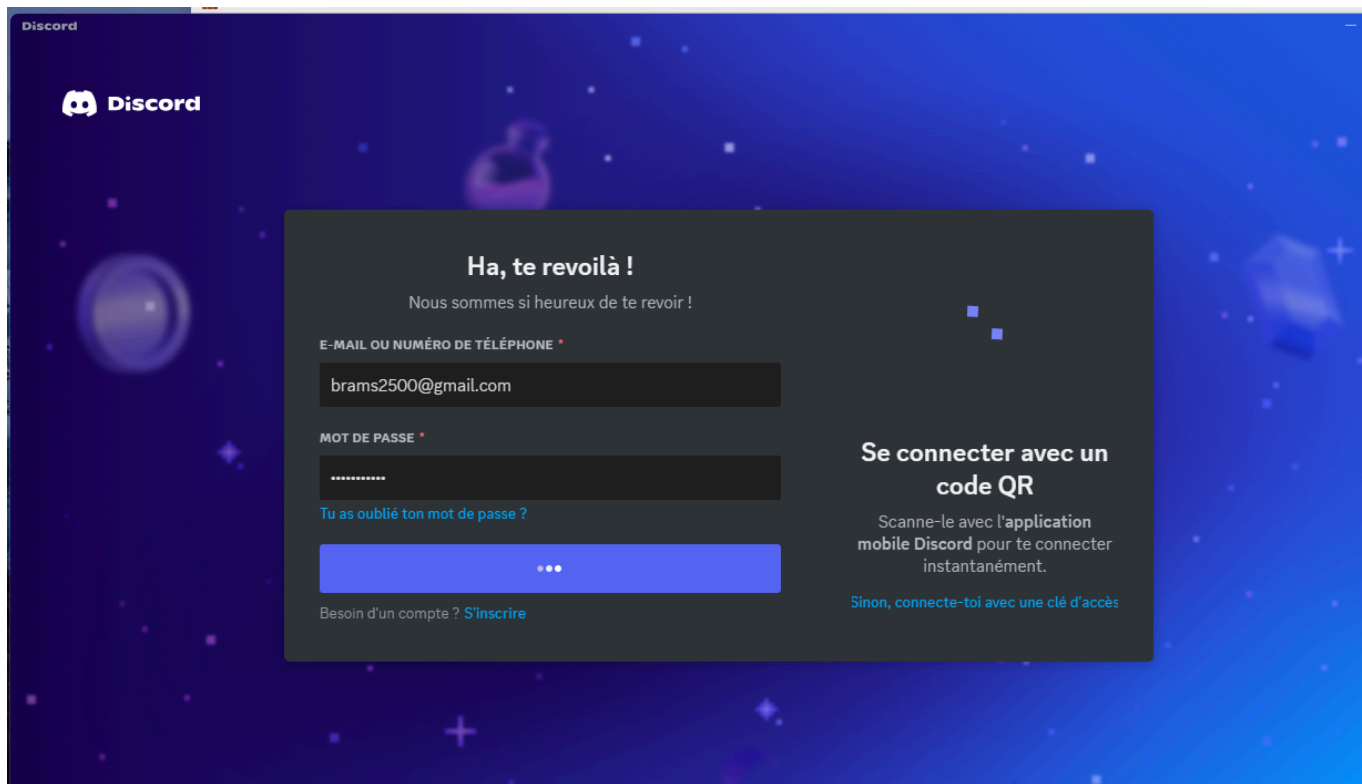
--> bloquer le port 443(HTTPS)



--> Action : Bloquer



--> la boucle tourne à l'infini



11 :

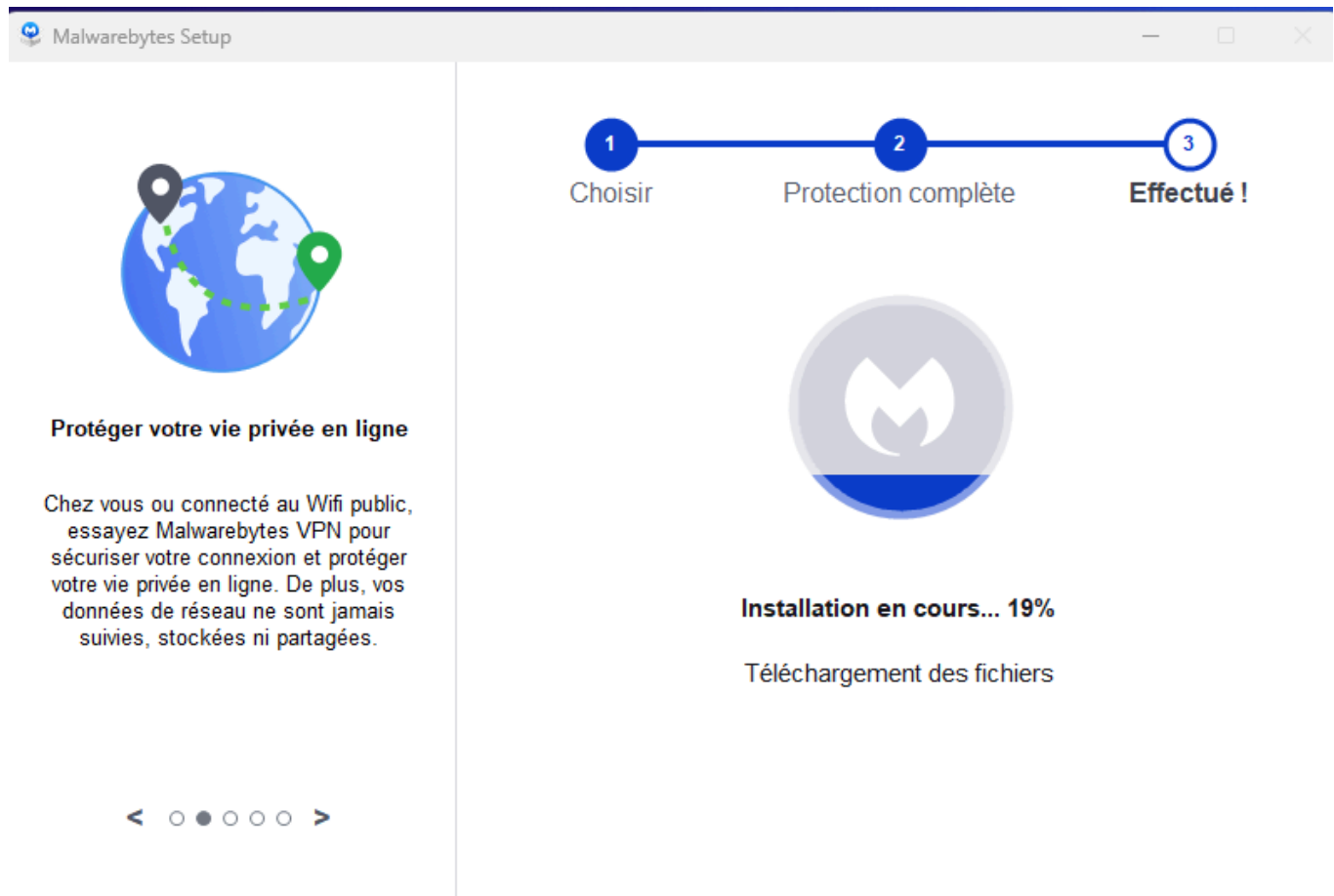
Conséquences d'un logiciel malveillant sur un poste peuvent être graves :

- Vol de données personnelles : Le malware peut voler des informations sensibles comme des mots de passe, des coordonnées bancaires ou des fichiers privés.
- Dommages au système\*\* : Il peut altérer ou détruire des fichiers système, rendant l'ordinateur instable ou inutilisable.
- Prise de contrôle à distance : Le malware permet à un attaquant de contrôler l'ordinateur à distance, l'utiliser pour des attaques ou l'intégrer à un réseau de machines compromises.
- Baisse de performance: Il peut ralentir l'ordinateur en consommant des ressources (processeur, mémoire, ...).
- Propagation sur le réseau: Il peut se propager à d'autres ordinateurs du réseau, affectant plusieurs machines.

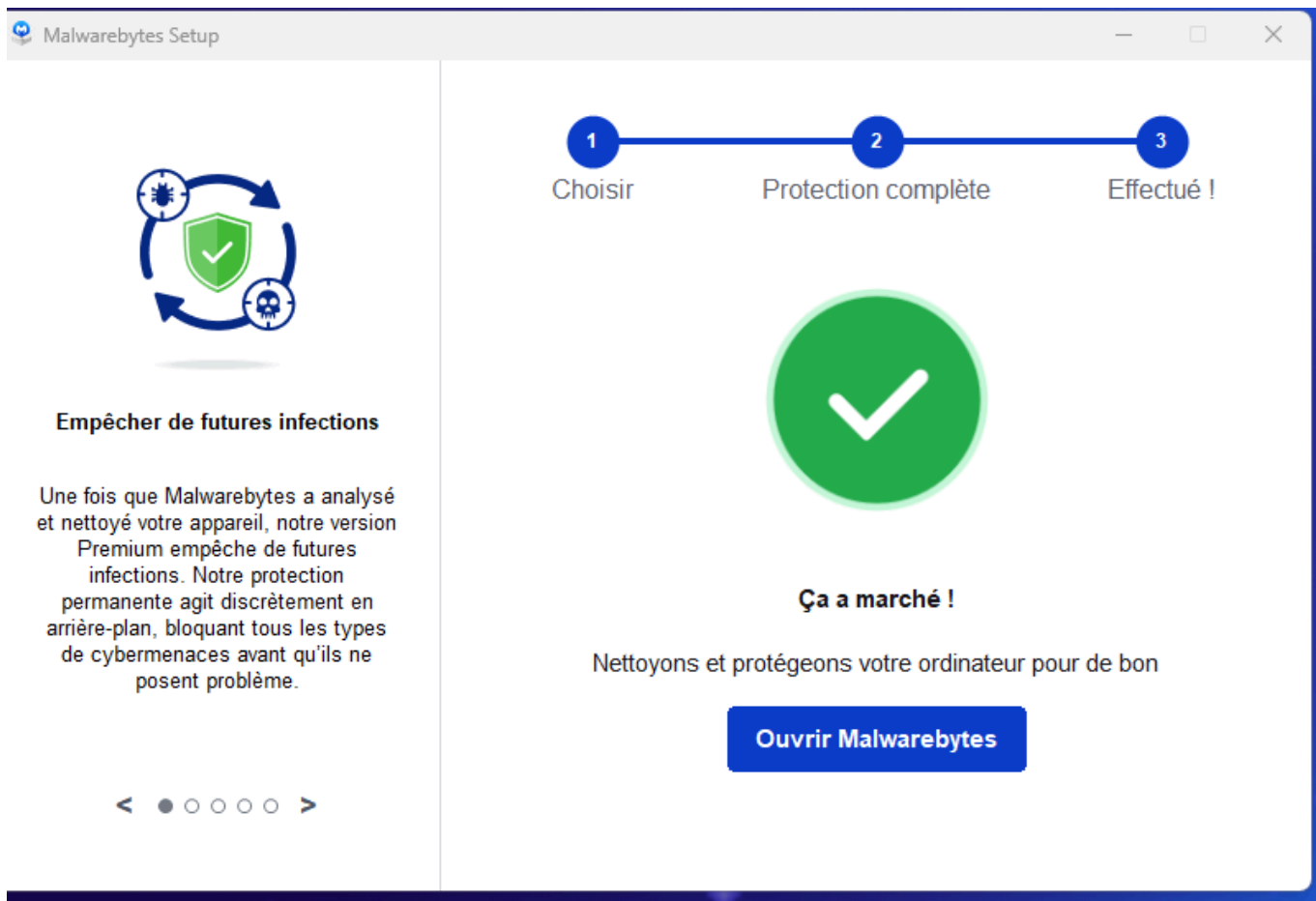
12 :

- SentinelOne
- Windows Defender
- AvastAntivirus
- esetAntivirus
- Norton Security


### 13: --> Installation de MalwareBytes











--> Lancement de l'analyse de mon appareil

 Malwarebytes




  
Analyse de l'appareil

  
Conseiller de confiance

  
Empreinte numérique

### Analyse de votre appareil à la recherche de menaces...





- ✓ Recherche de mises à jour
- Analyse de la mémoire
- Analyse des éléments de démarrage
- Analyse du système de fichiers


| Durée d'analyse | Éléments analysés | Détections |
|-----------------|-------------------|------------|
| 0:00:10         | 107               | 0          |


Mettre en pause l'analyse de l'appareil


Ignorer l'analyse de l'appareil

 Malwarebytes




  
Analyse de l'appareil

  
Conseiller de confiance

  
Empreinte numérique

### Bonne nouvelle, aucune menace n'a été détectée



Ensuite, notre Conseiller de confiance vérifiera s'il y a des failles dans votre sécurité

Suivant



Analyse de l'appareil



Conseiller de confiance



Empreinte numérique

## Voici ce que nous avons trouvé



### Windows n'est plus à jour

Les mises à jour Windows apportent des améliorations essentielles en matière de sécurité et de performances



### Pare-feu activé

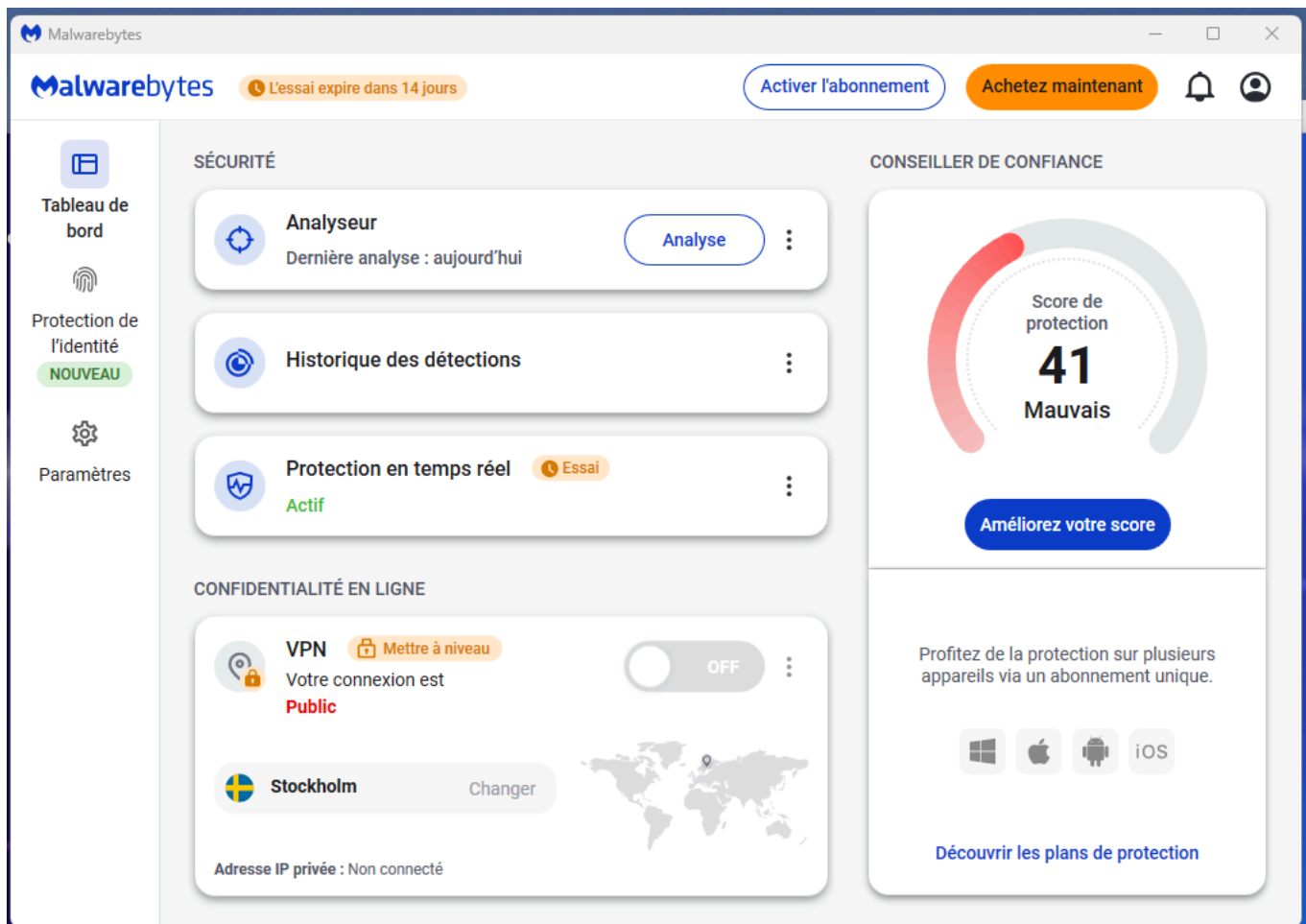
Bloque les attaques réseau et les accès non autorisés

Ne vous inquiétez pas, nous vous aiderons à résoudre ces problèmes plus tard.

Ensuite, nous effectuerons une recherche sur le dark web à la recherche d'informations divulguées ou volées vous concernant.

Suivant

--> Tableau de bord de malwarebytes



14:

-Détection et analyse : détecte les malwares (virus, ransomwares, spywares, etc.) en utilisant des bases de données de signatures et en analysant les comportements suspects.

-Protection en temps réel : surveille constamment l'ordinateur pour repérer toute activité anormale et bloque immédiatement les menaces.

-Suppression des malwares : Une fois les malwares trouvés, il les supprime ou les met en quarantaine pour les empêcher d'endommager le système.

-Protection contre les exploits : bloque les tentatives d'exploitation de failles dans les logiciels avant qu'elles ne causent des dégâts.

15: Non, je suis étudiant, j'ai juste vu les paramétrages de bases d'un pare-feu Stormshield.