Mr JACQUEMIN

19/03/2024

Compte rendu TP

Initialisation au Pare-Feu

TEWES Arnaud
BTS SIO SISR 1ERE ANNEE

1. Introduction au pare-feu

1. Un Pare-Feu est un équipement informatique de sécurité qui permet de filtrer le trafic entrant, sortant et à l'intérieur d'un réseau informatique. Cet équipement permet de bloquer ou d'autoriser les paquets de données. Son rôle est d'agir comme une barrière entre le réseau interne et le réseau externe grâce a des règles que nous lui définissons.

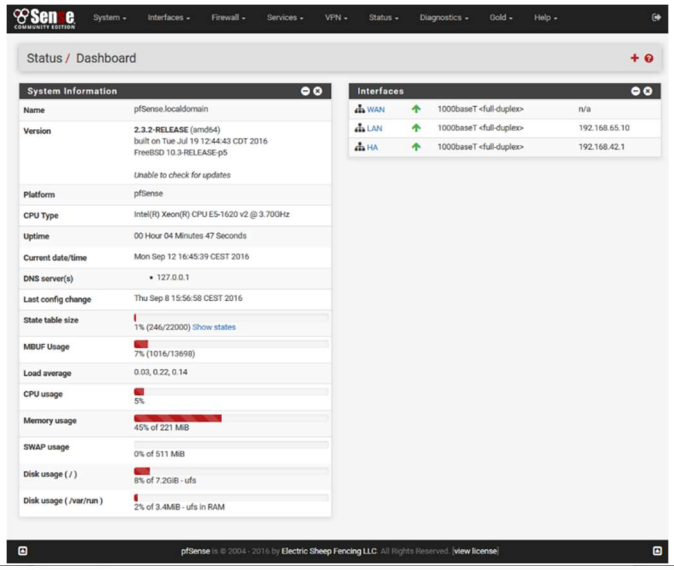
2. Les deux catégories principales d'un pare-feu sont :

- Le pare-feu logiciel : C'est une application (ou image) que l'on installe sur un serveur ou un ordinateur et qui a l'avantage d'être plus flexible (idéal pour un particulier)

- Le pare-feu physique : c'est un équipement physique semblable à un routeur mais qui à pour rôle de filtrer directement à l'entrée du réseau interne. Il offre une protection plus robuste qu'un pare-feu logiciel (idéal pour une entreprise)

Pare-feu physique

Pare-feu logiciel



3. Avantages et inconvénients d'un pare-feu logiciel et d'un pare-feu matériel :

Pare-feu Matériel :

Avantages :

- Sécurité : Le pare-feu matériel offre une protection physique entre le réseau interne et le réseau externe. Il est placé juste après le routeur (ou la box internet) et permet de filtrer directement à l'entrée du réseau interne
- Performance : Ils sont conçus pour gérer un plus grand volume de trafic réseau
- Ils sont simples à mettre en place et à configurer

Inconvénients

- Coût : Il est plus couteux à l'achat et à la maintenance
- Moins de flexibilité : Leurs déploiement est plus complexe qu'un pare-feu logiciel

Pare-feu logiciel :

Avantages :

- Flexibilité : Ils peuvent être installé sur n'importe quelle machine, serveur ou VM
- Cout réduit : Ils sont moins cher qu'un pare-feu matériel et permettent une maintenance plus simple

Inconvénients :

- Moins performants, ils ne peuvent pas gérer un trafic réseaux élevé
- Ils ne sont directement placés à l'entrée du réseau et ne fournissent pas une sécurité aussi élevé qu'un pare-feu matériel
- Ils sont directement installés sur une machine et sont donc dépendant de la machine sur laquelle ils sont installé

2. Le Pare-feu Windows

4. Les principales fonctionnalités du pare-feu Windows (pare-feu logiciel) est de :

- Filtrer le trafic réseau entrant et sortant de LA MACHINE sur laquelle il est installé.
- Bloquer ou autoriser les accès en provenance ou vers un port de son appareil
- Bloquer les connexions provenant ou vers une adresse IP spécifique
- Autoriser l'accès au réseau à une application en particulier

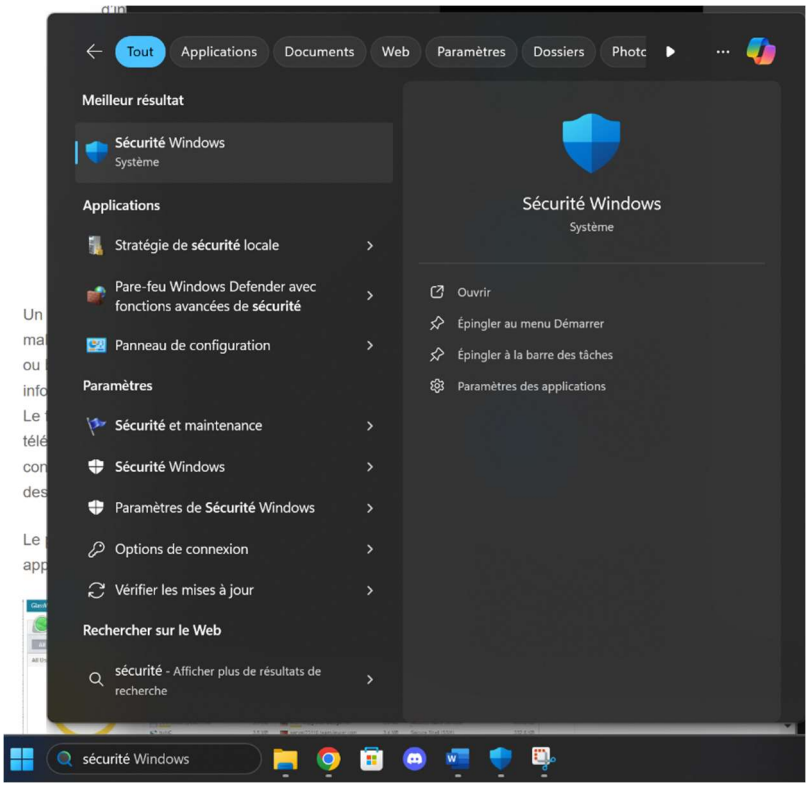
Un pare-feu permet donc de protéger des connexions entrantes malveillants, comme des scans provenant de l'extérieur (souvent internet) ou bloquer les tentatives d'accès à son réseau interne

Le filtrage des connexions sortantes permet d'empêcher ou limiter le téléchargement et installation de logiciels malveillants

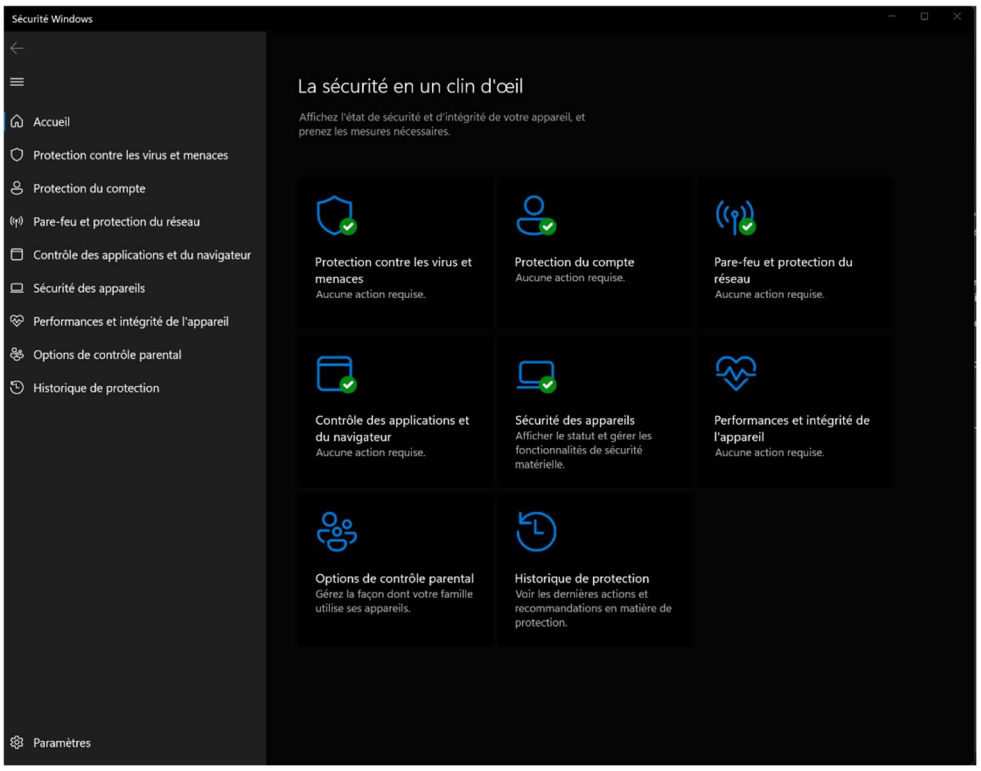
Le pare-feu sur Windows analyse en permanence l'activité des applications afin d'autoriser ou non les connexions réseaux.

5. Pour désactiver le Pare-feu sur Windows, il faut se rendre dans sécurité Windows via le panneau de configuration ou comme suit :

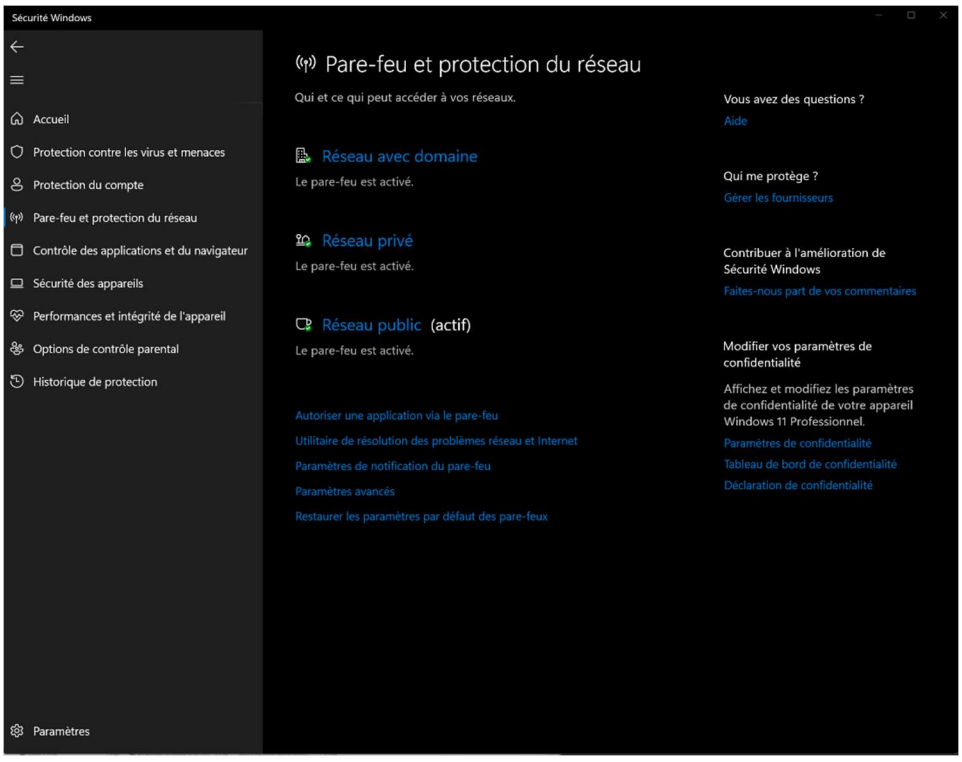
Tapez dans la barre de recherche « sécurité Windows »



Ensuite dans la console de gestion, on retrouve « Pare-feu et protection du réseau » sur la droite



Nous pouvons ensuite en entrant dans chaque catégorie, désactiver tous les types de pare-feu (nécessite des droits administrateur)



6. Dans le Pare-feu Windows, la différence entre les trois types de pare feu sont :

Réseau avec domaine : Prend en charge les règles de pare-feu mise en place dans le domaine dans laquelle la machine se trouve (souvent stricte, pour un réseau d'entreprise par exemple)

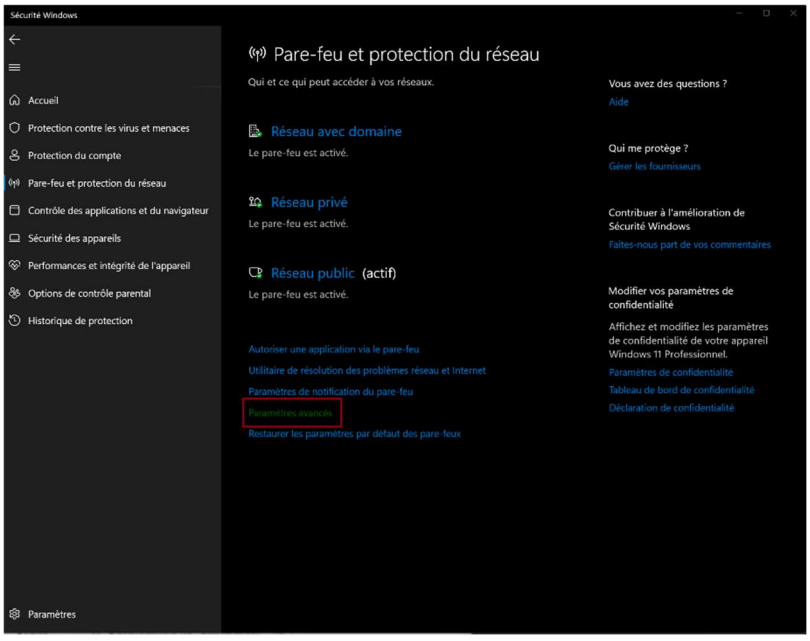
Réseau privé : Prend en charge les règles de réseau pour un réseau privé et interne (moins stricte, laisse la découverte réseau active et permet le partage de fichiers entre les différente machines)

Réseau public : Le réseau public quant-à-lui permet de bloquer la découverte réseau sur un réseau non sécurisé (comme le Wi-Fi d'un endroit public, restaurant, etc.) et bloque l'accès à toute les machines sur le même réseau à son appareil

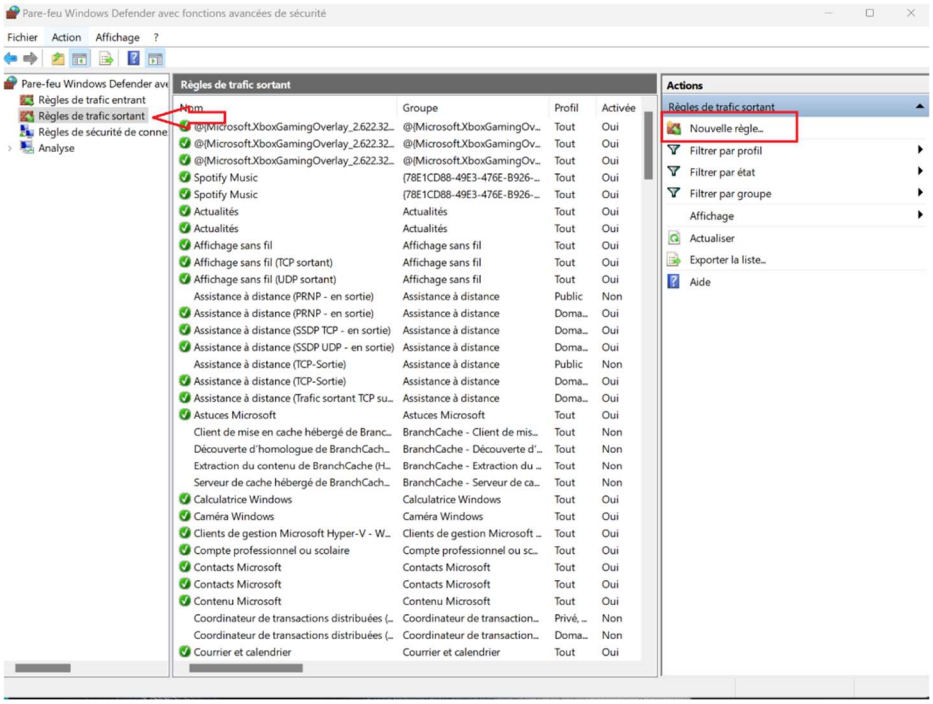
7. Pour le moment, ma machine est dans un réseau public car je suis connecté à mon téléphone en partage de connexion. Dans l'éventualité ou d'autre personnes de ma classe aurait accès à mon partage (mot de passe non sécurisé), je l'ai mis dans ce type de réseau pour pouvoir rester sécurisé lors de ma navigation.

8. Une règle de pare-feu est une règle que l'on défini sur son pare-feu et qui permet de bloquer ou d'autoriser du trafic réseau et de gérer les conditions pour que cela se produise.

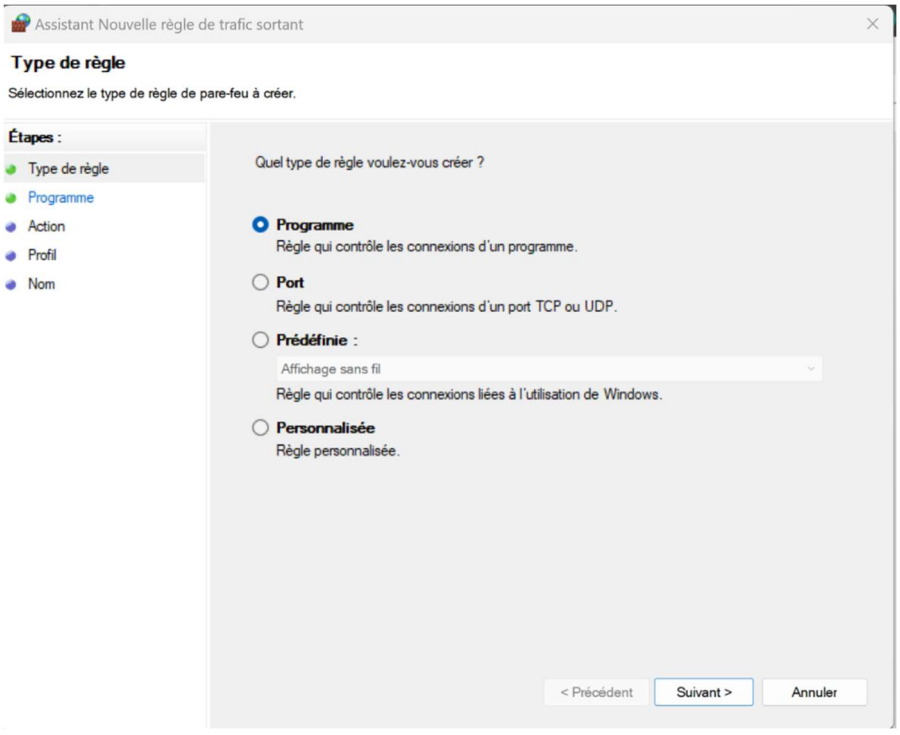
Pour créer une règle sur le pare-feu Windows, il faut se rendre dans le pare-feu Windows, puis dans paramètres avancés :



Ensuite il faut aller dans l'onglet « règle de trafic sortant » ou « entrant » et cliquer sur « nouvelle règle »



Maintenant, nous avons la possibilité de créer une règle selon si l'on veut bloquer une application, un port ou autre.



9. Quelle est la différence entre une règle entrante et une règle sortante ?

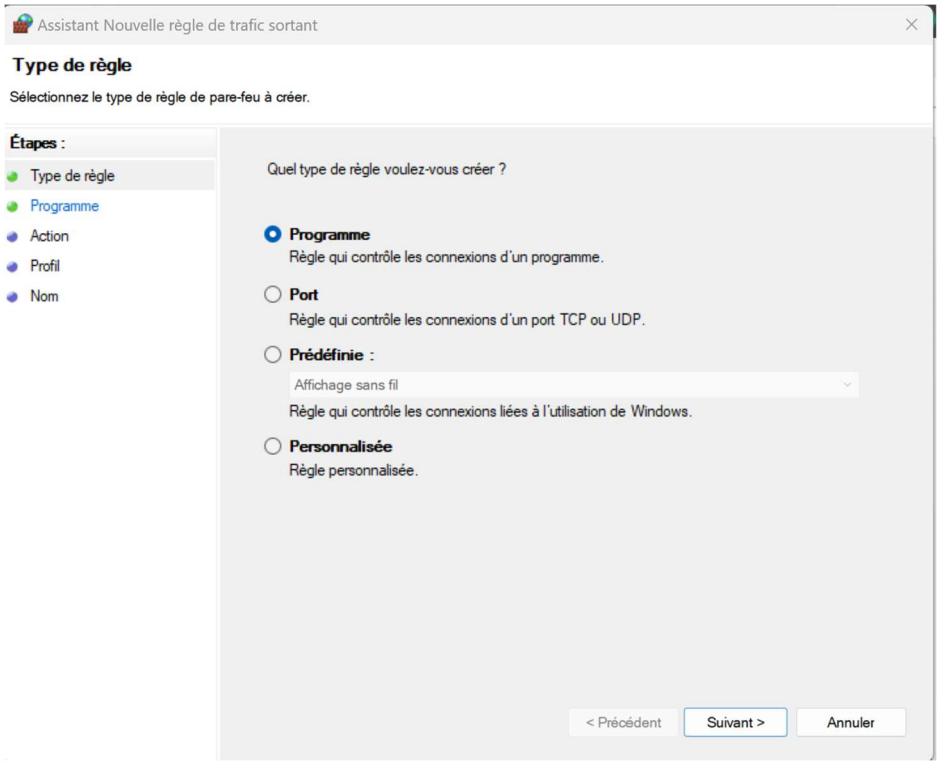
- Les règles sortantes : gèrent le trafic qui quitte votre ordinateur et se dirige vers le réseau externe

- Les règles entrantes : gèrent le trafic qui arrive sur votre ordinateur depuis le réseau externe (par exemple, Internet)

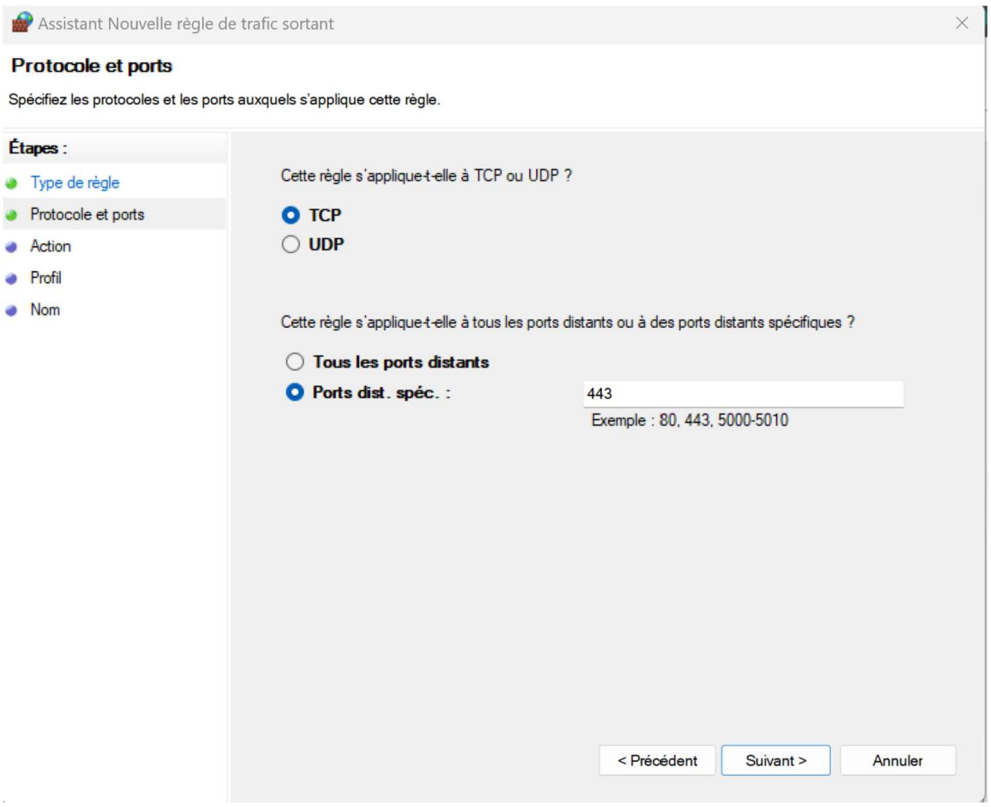
10. Pour créer une règle pour bloquer discord, nous avons deux options : soit de bloquer le port 443 (https), soit de bloquer directement l'exécutable de discord (lorsque cela fonctionne)

Pour ce test, je vais bloquer directement le port 443 (ce qui va bloquer l'accès à tout les sites web et application utilisant ce protocole).

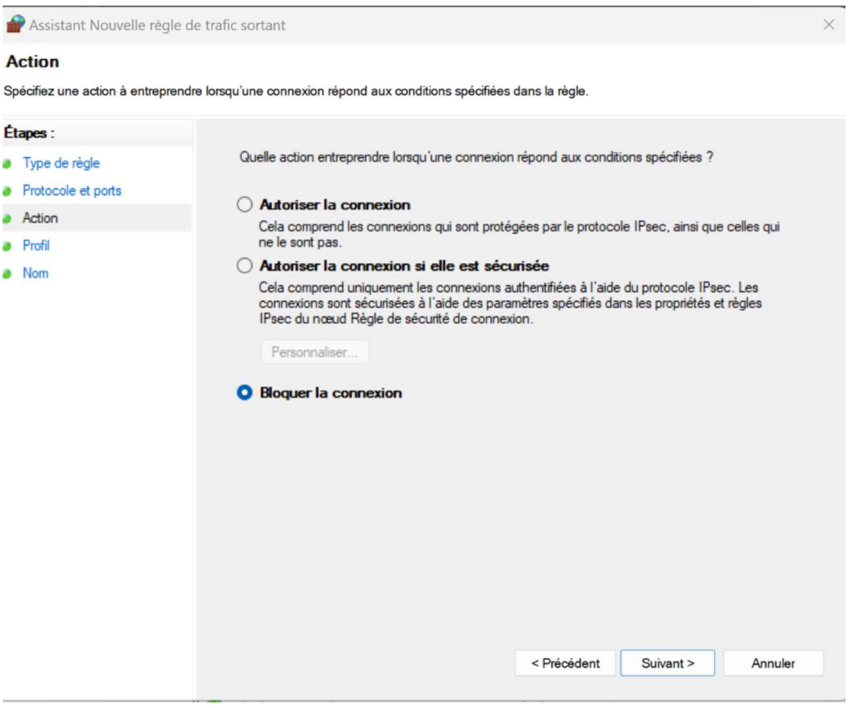
Comme vu précédemment, nous créons la nouvelle règle et choisissons l'options « port » :



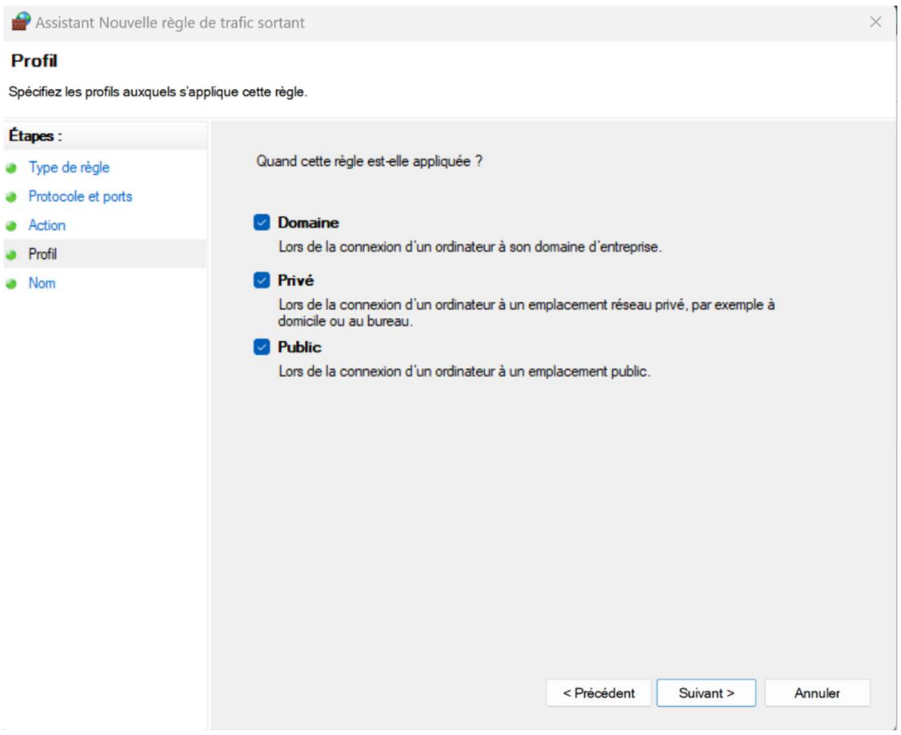
Ensuite, il faut choisir le protocole et définir le port à bloquer.



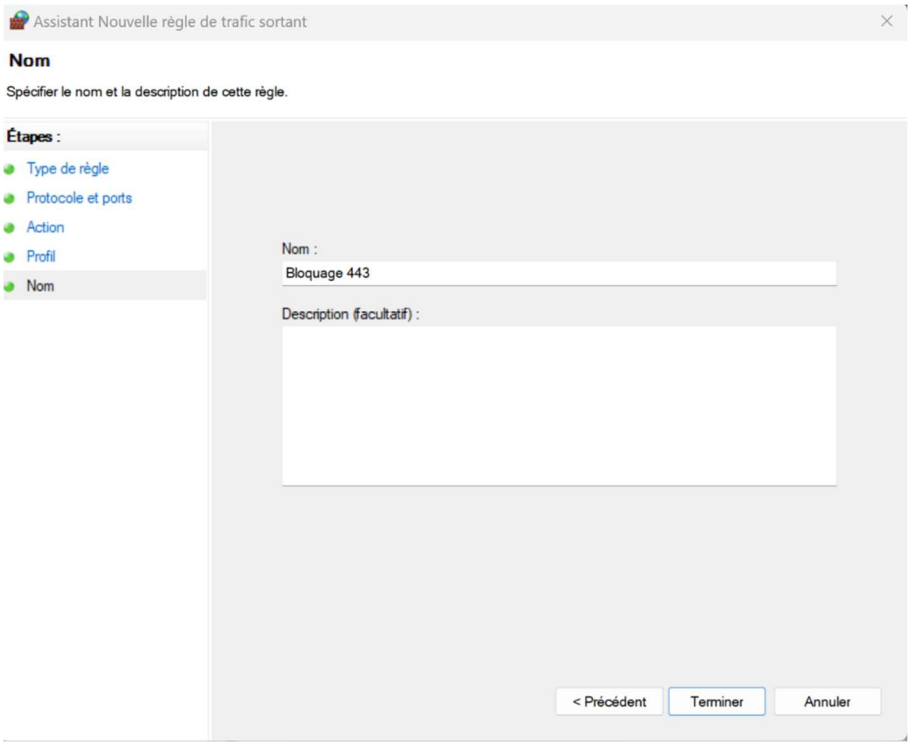
Maintenant, il faut définir si l'on veut bloquer ou autoriser la connexion à ce dernier.



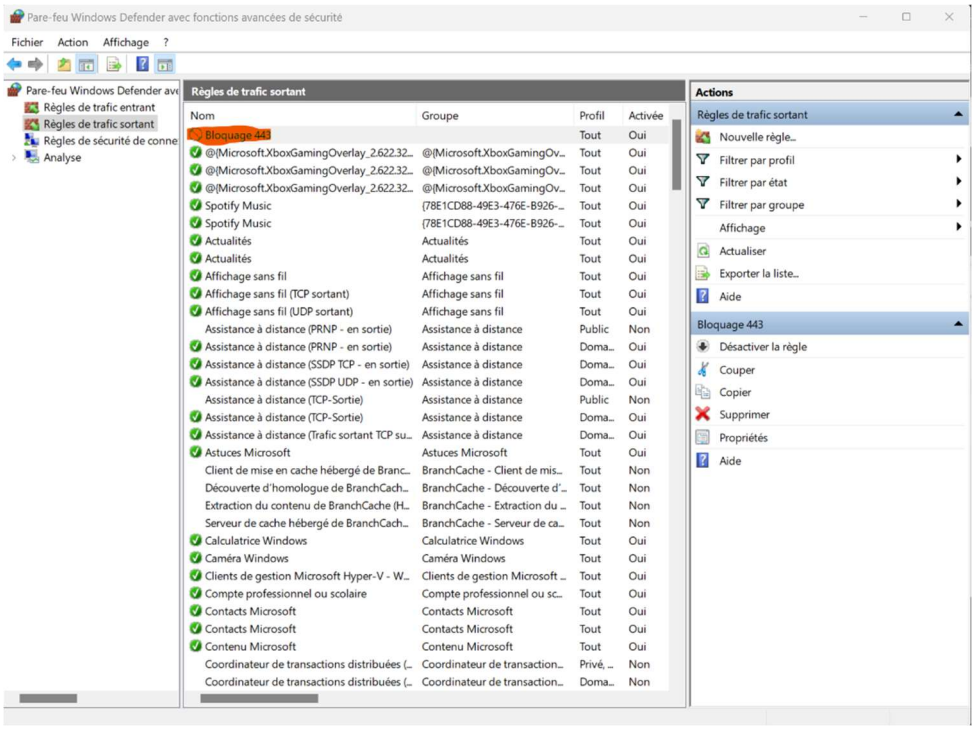
Il faut maintenant définir sur quel type de pare-feu l'on veut que notre règle s'applique :



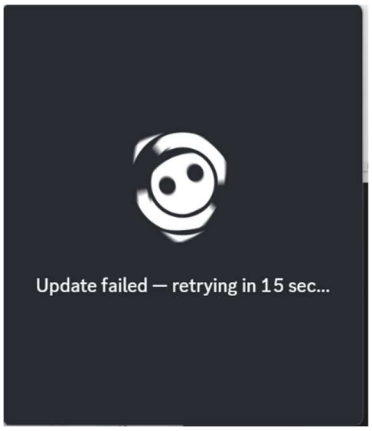
Nous avons la possibilité lui mettre un nom si nous le voulons pour pouvoir la retrouver.



La règle est maintenant créée. Je vais essayer d'ouvrir discord pour voir si cela fonctionne :



Il m'est impossible de me connecter au client discord, et il ne peut pas effectuer les mises à jour.



3. Désinfection des Logiciels Malveillants

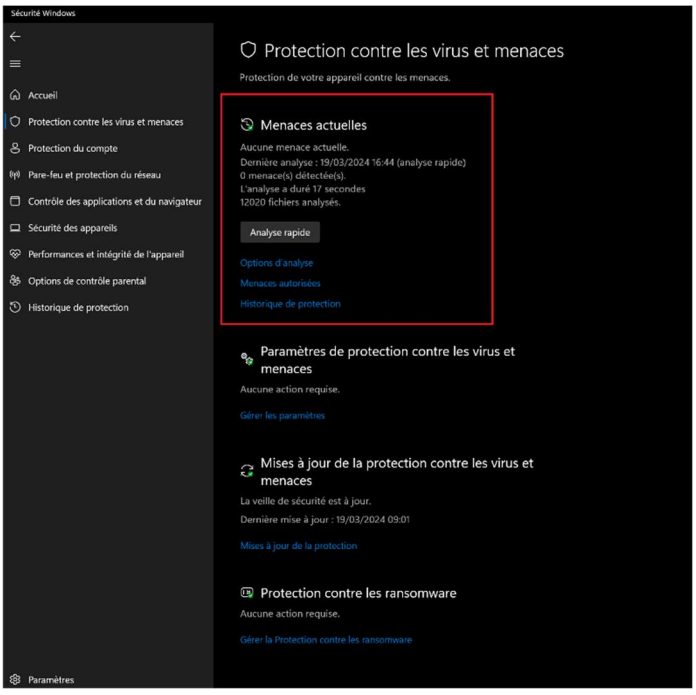
11. Les logiciels malveillants peuvent avoir des conséquences néfastes sur un poste comme :

- **Perte de données** : Les logiciels malveillants peuvent corrompre, supprimer ou voler des fichiers et documents.
- **Ralentissement du système** : Ils peuvent consommer des ressources système, entraînant un fonctionnement plus lent d'un ordinateur.
- **Vol d'informations personnelles** : Certains logiciels malveillants sont conçus pour voler des informations sensibles telles que les mots de passe, les numéros de carte de crédit, etc.
- **Propagation à d'autres appareils** : Si un logiciel malveillant infecte un poste, il peut également se propager à d'autres appareils connectés au même réseau.

12. Voici trois outils de désinfection que vous pouvez utiliser pour protéger votre poste :

- **Microsoft Defender Antivirus** : Cet outil intégré à Windows 10 et 11 recherche et supprime les programmes malveillants.
- **Malwarebytes** : Un outil populaire pour détecter et supprimer les logiciels malveillants
- **AdwCleaner** : Cet outil cible les adwares et les programmes potentiellement indésirables

13. J'ai exécuté l'outil de Windows Microsoft Defender en analyse rapide (il existe d'autre options comme une analyse complète ou une personnalisée)



14. Les logiciels malveillants fonctionnent de différentes manières :

- **Virus** : Ils s'attachent à des fichiers exécutables et se propagent lors de l'exécution de ces fichiers
- **Vers** : Ils se répliquent et se propagent automatiquement via les réseaux
- **Chevaux de Troie** : Ils se font passer pour des logiciels légitimes, mais ont des intentions malveillantes
- **Adwares** : Ils affichent des publicités indésirables
- **Ransomwares** : Ils chiffrent vos fichiers et demandent une rançon pour les débloquer

Avis personnel

15. Dans le cadre de mon alternance, j'ai eu l'occasion d'observer comment mes collègues paramétraient et installaient des pare-feux. J'ai également vu mon collègue devoir appeler le service client Orange lorsque nous installions un pare-feu dans une entreprise où il y a une Livebox Business (car nous ne pouvons pas prendre la main sur la box). L'objectif était de mettre en place la DMZ et de nous fournir un pool d'adresses IP publiques pour configurer le pare-feu.

    J'ai également assisté à la configuration des règles du pare-feu en production avant l'installation chez nos clients. Malheureusement, je n'ai pas encore eu l'occasion de manipuler un pare-feu moi-même.

16. Plus jeune, j'ai été confronté à un "malware" lorsque j'ai voulu tricher à un jeu en ligne. J'ai pu profiter d'un Mod Menu lors de mes parties en ligne, mais j'ai ensuite dû réinitialiser tout mon PC. En effet, ce logiciel contenait également un logiciel malveillant, et Microsoft Defender s'est emballé, rendant mon poste inutilisable (le CPU était constamment surchargé). Par la suite, j'ai appris grâce au forum d'entraide Malekal qu'il existait d'autres moyens d'agir et surtout d'empêcher l'intrusion de logiciels malveillants sur son poste, mais je l'ai malheureusement su après coup.

    Malekal, en scannant un ordinateur avec un de leurs outils et en leurs postant le rapport, sont capable de nous dire si oui ou non un malware est présent, mais en plus nous aide pour le supprimer et nous donnent des conseils pour ne plus que cela arrive.

    C'est une communauté super que je recommande !