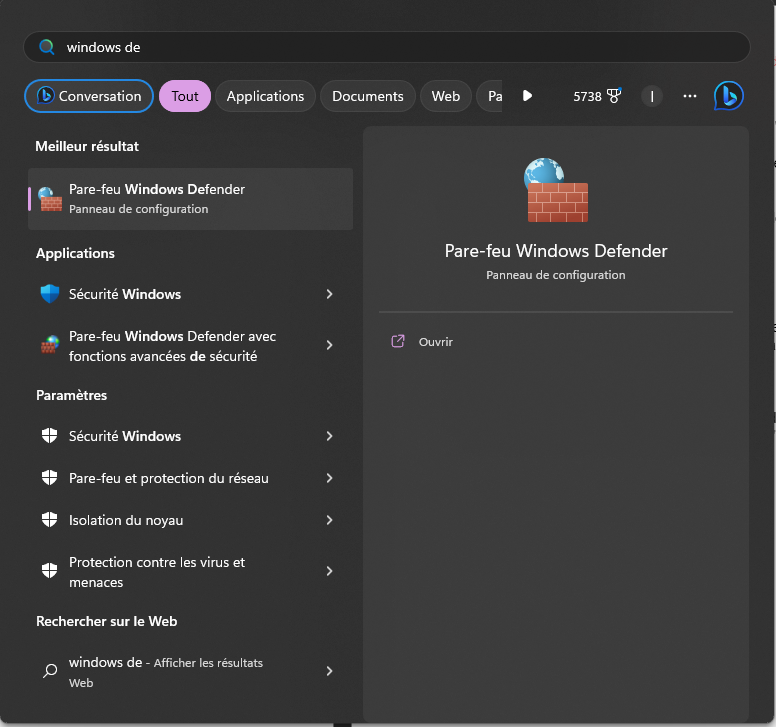
|  |
| --- |
| **Exercice : Filtrage des connexions Windows**  Vous allez paramétrer Windows Defender pour le filtrage suivant  **Les connexions sortantes**   * tous les accès en sortie de votre poste sont bloquées à l’exception des accès aux réseau 192.168.3.0/24   **Les connexions entrantes :**   * Le poste doit répondre aux requêtes ping ( ICMP) * Le poste doit permettre la prise en main bureau distant depuis un poste de votre réseau. * Toutes les autres connexions entrantes sont bloquées |

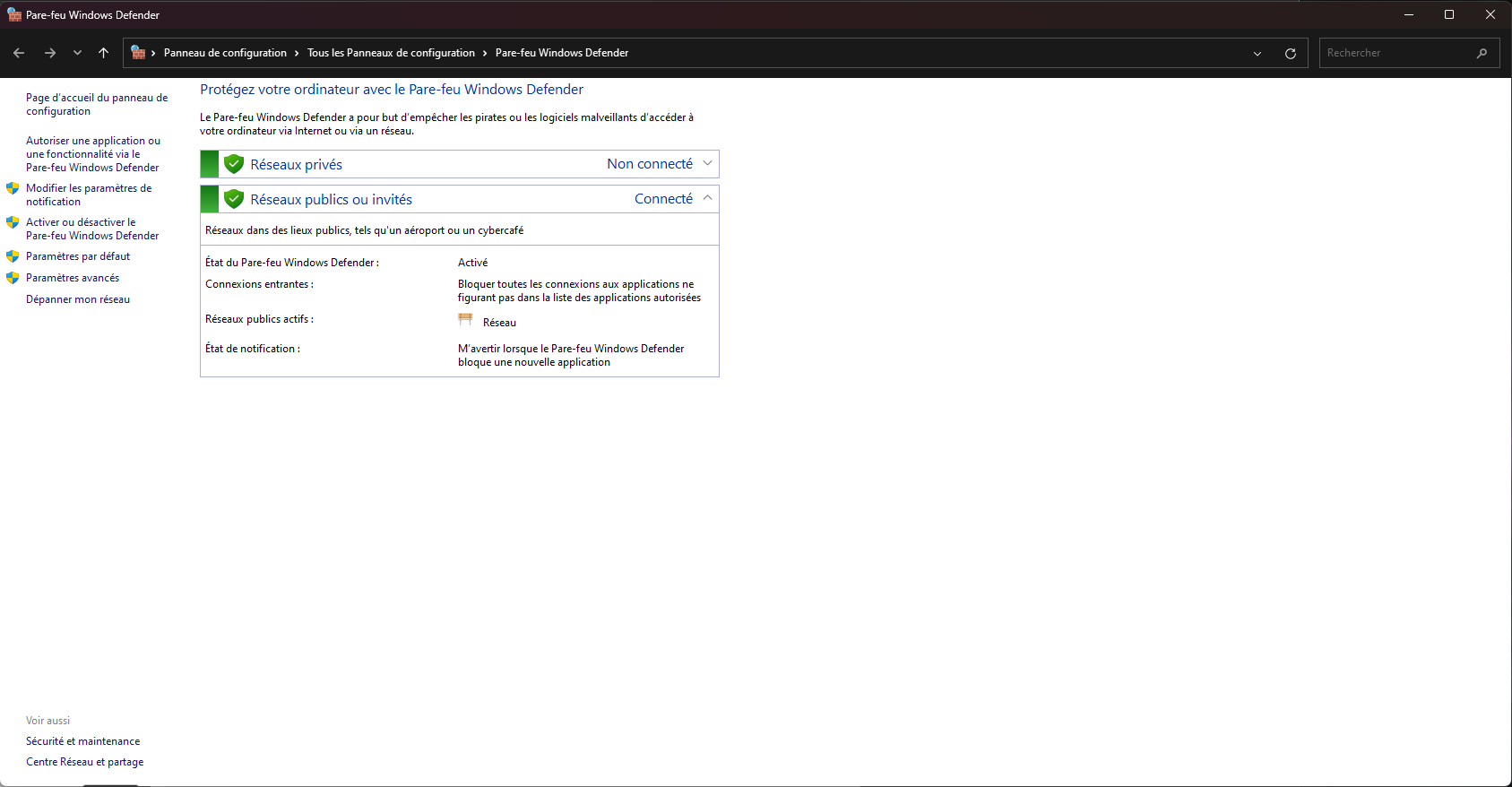
Bloquer tous les accès en sortie de votre poste est bloquées à l’exception des accès aux réseau 192.168.3.0/24

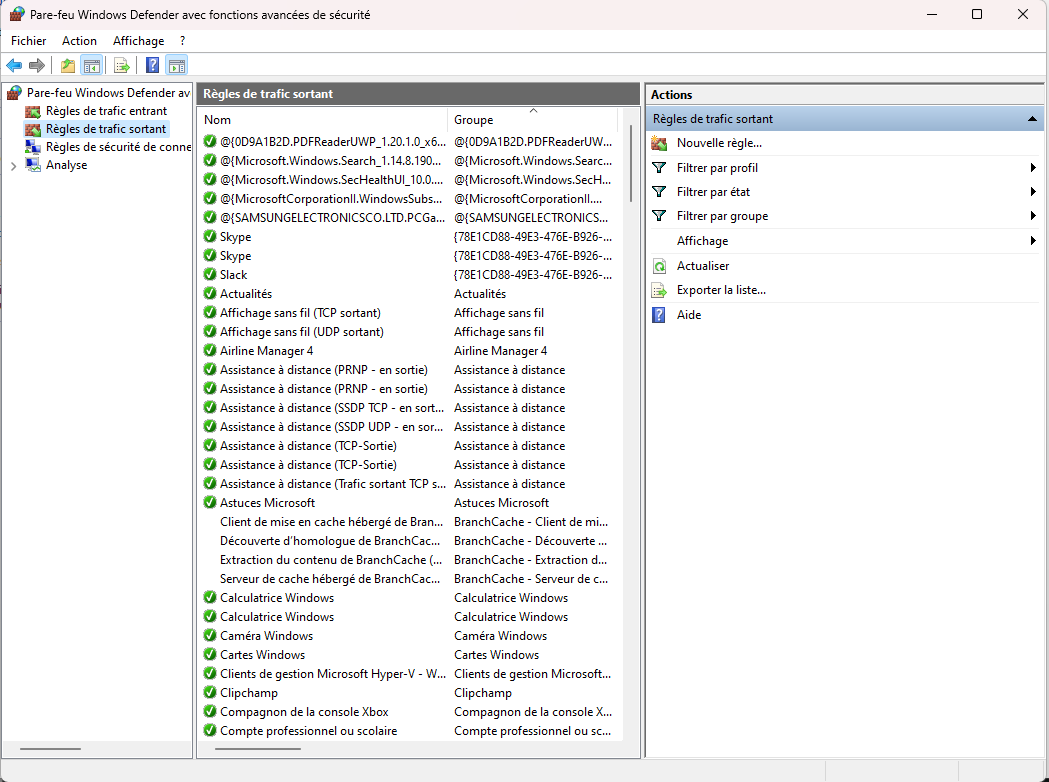
Voici comment paramétrer Windows Defender pour le filtrage des connexions sortantes comme spécifié :

Tout d'abord, ouvrez Windows Defender en cliquant sur le bouton "Démarrer" de Windows, en tapant "Windows Defender" dans la barre de recherche et en sélectionnant l'application "Windows Defender Firewall avec des fonctions avancées de sécurité".

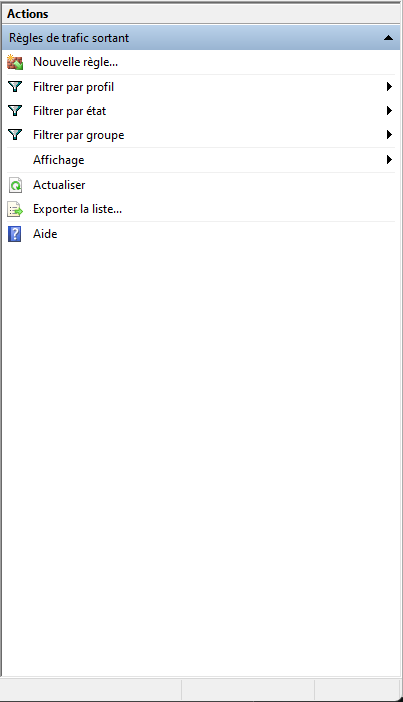


Dans la fenêtre de Windows Defender, cliquez sur "Paramètres avancés" dans le volet de gauche.

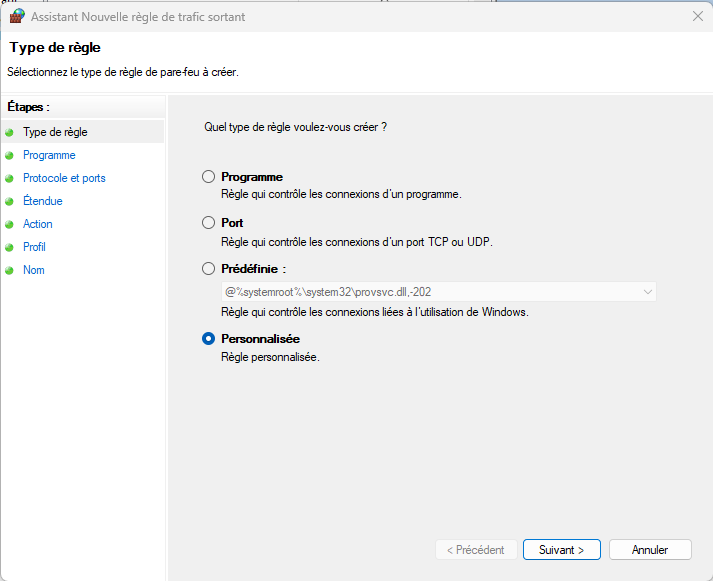


Dans la fenêtre de Windows Defender, cliquez sur "Règles de trafic sortant" dans le volet de gauche.

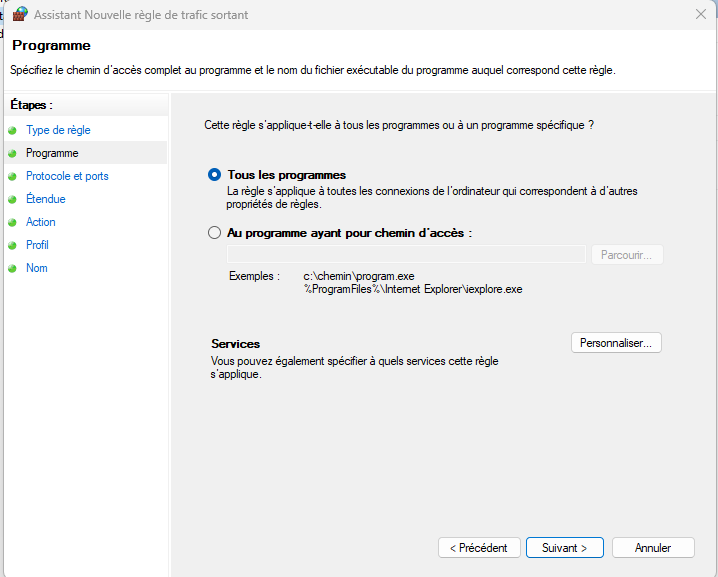
Cliquez sur "Nouvelle règle..." dans le volet de droite.



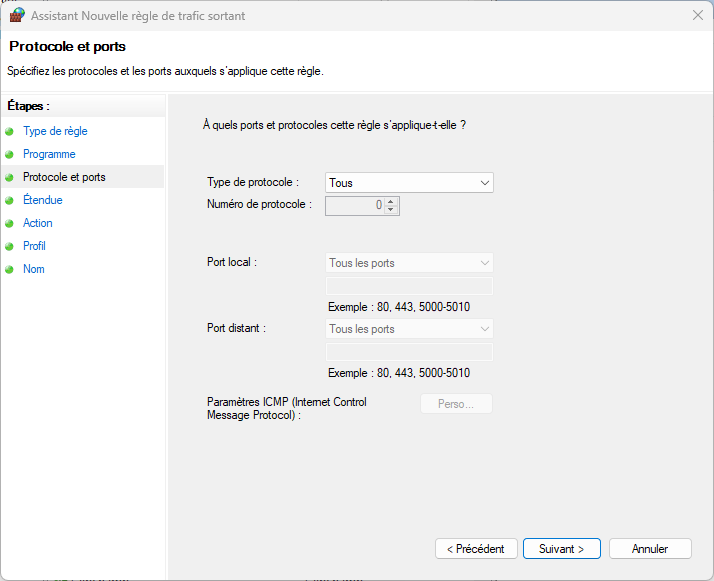
Dans la boîte de dialogue qui s'affiche, sélectionnez "Personnalisée" et cliquez sur "Suivant".



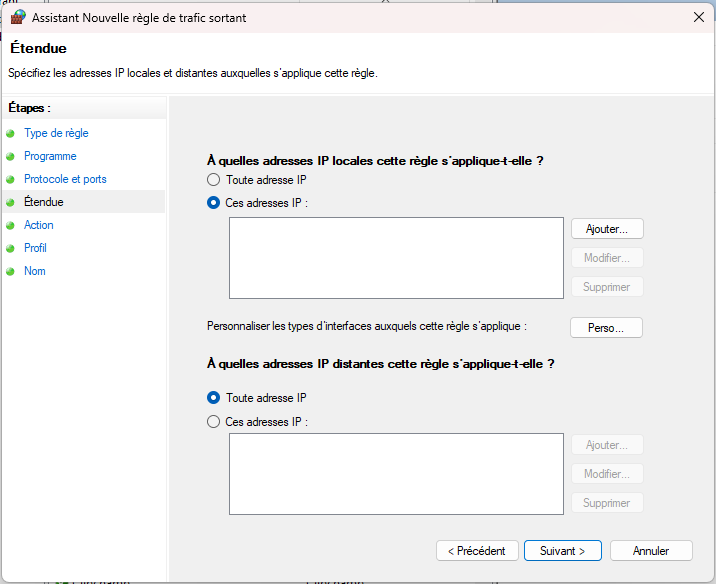
Sélectionnez « tous les programme » pour bloquer les connexions sortantes.



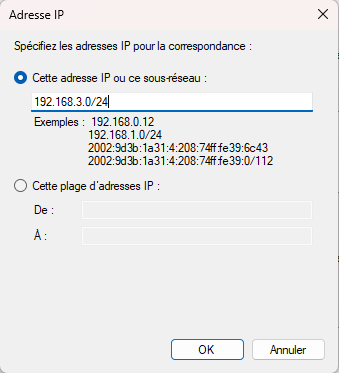
Dans la boîte de dialogue "Protocoles et ports", sélectionnez "Tous les ports" et cliquez sur "Suivant".



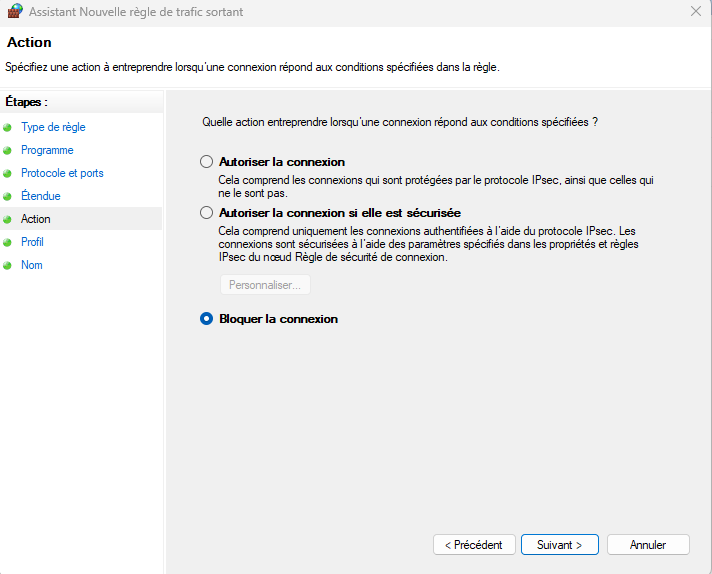
Dans la boîte de dialogue "Etendue", sélectionnez "Ces adresses IP" et cliquez sur "Ajouter...".



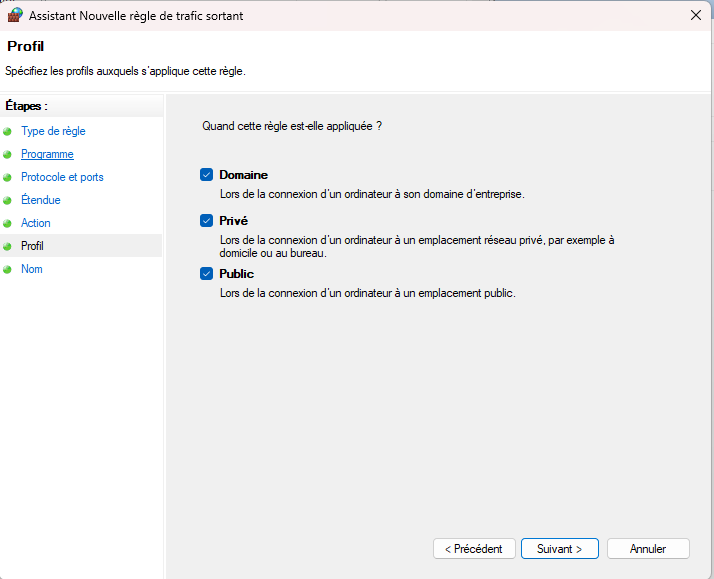
Dans la boîte de dialogue "Adresse IP", sélectionnez "Ces adresses IP" et entrez "192.168.3.0/24" dans le champ « Cet ensemble d'adresses IP ». Cliquez sur "OK", puis sur "Suivant".



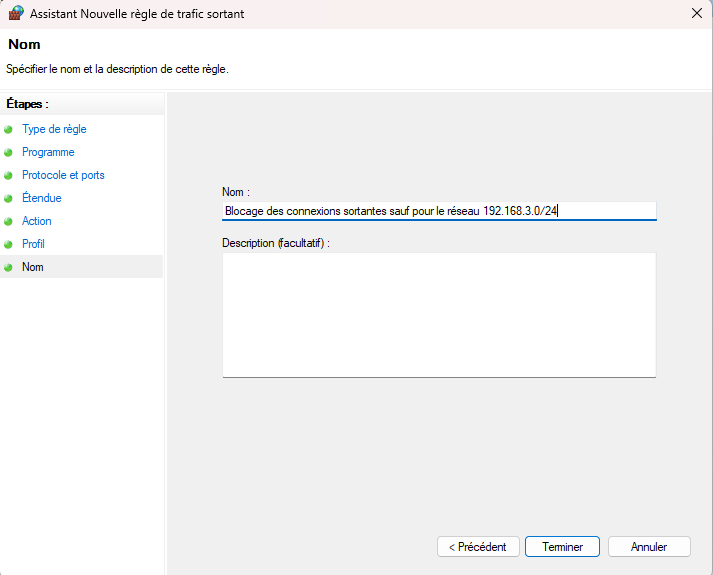
Sélectionnez "Bloquer la connexion" et cliquez sur "Suivant".



Cochez les cases correspondant aux profils de réseau pour lesquels vous voulez bloquer les connexions sortantes, puis cliquez sur "Suivant".

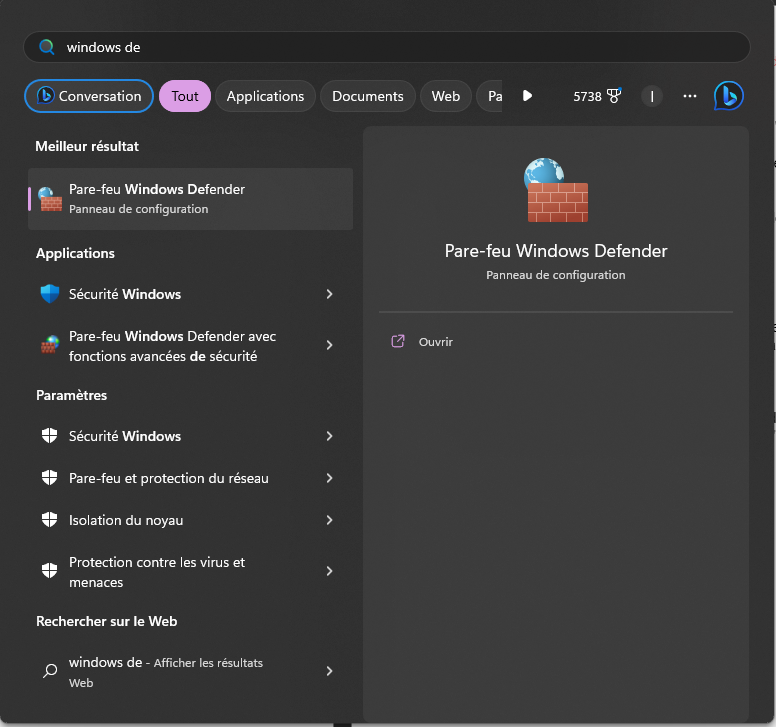


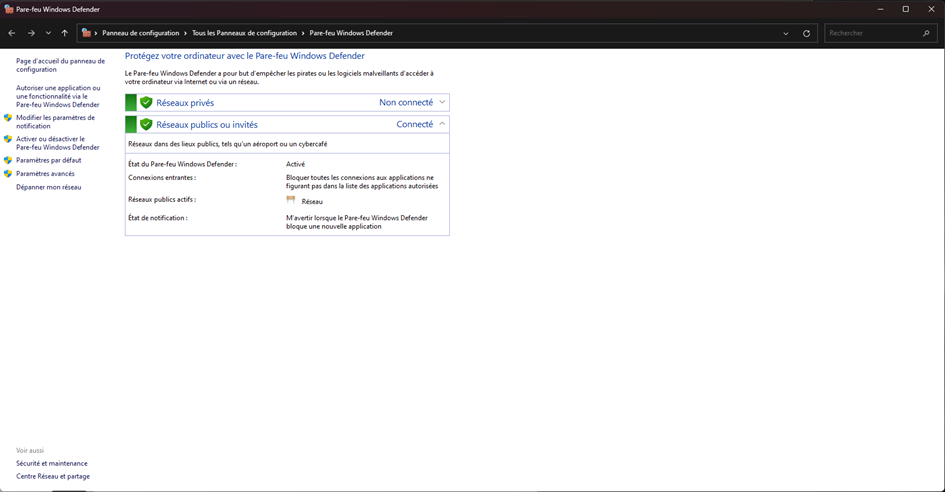
Donnez un nom à la règle, "Blocage des connexions sortantes sauf pour le réseau 192.168.3.0/24", puis cliquez sur "Terminer".

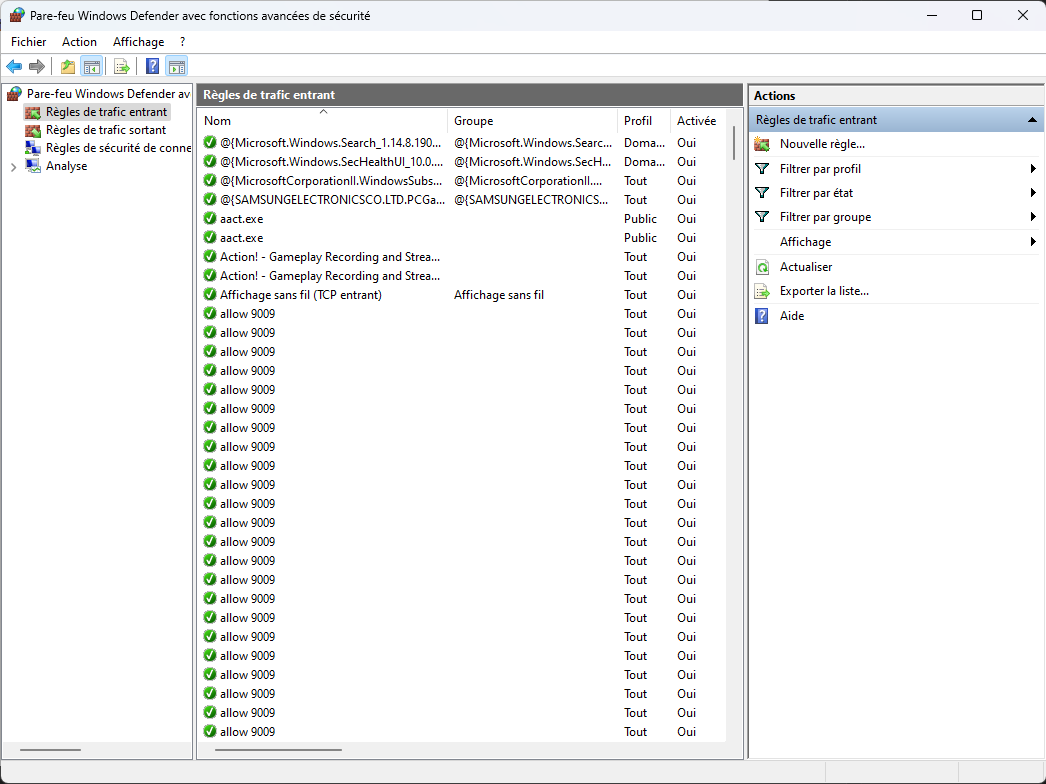


Le poste doit répondre aux requêtes ping ( ICMP)

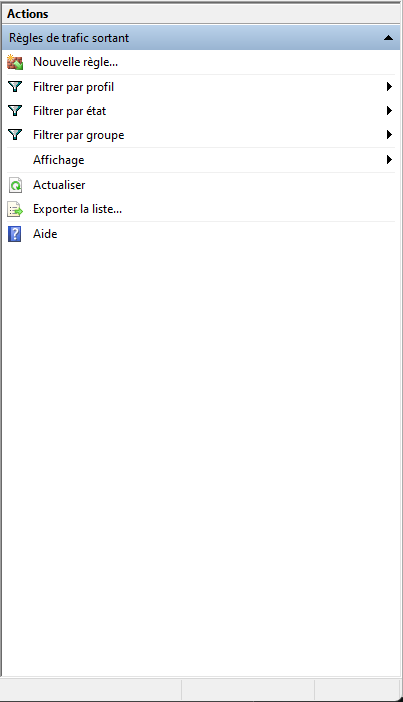
Voici comment paramétrer Windows Defender pour permettre les connexions entrantes de type ping (ICMP) :

Tout d'abord, ouvrez Windows Defender en cliquant sur le bouton "Démarrer" de Windows, en tapant "Windows Defender" dans la barre de recherche et en sélectionnant l'application "Windows Defender Firewall avec des fonctions avancées de sécurité".

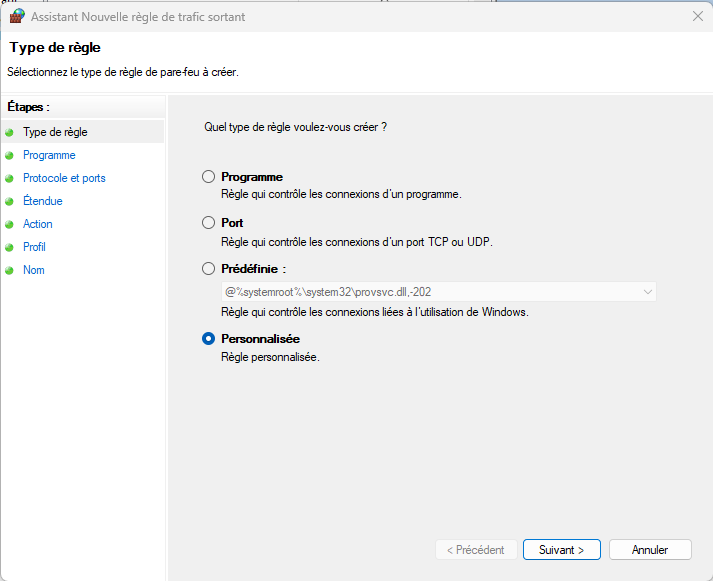
Dans la fenêtre de Windows Defender, cliquez sur "Paramètres avancés" dans le volet de gauche.

Dans la fenêtre de Windows Defender, cliquez sur "Règles de trafic sortant" dans le volet de gauche.

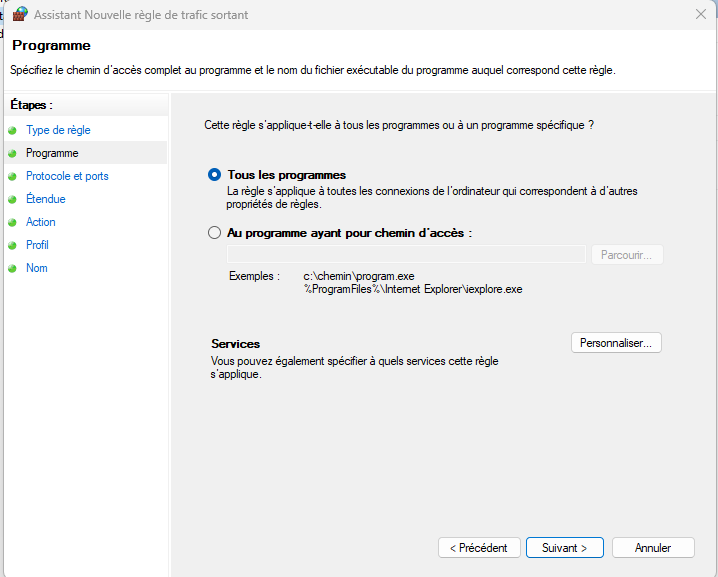
Cliquez sur "Nouvelle règle..." dans le volet de droite.



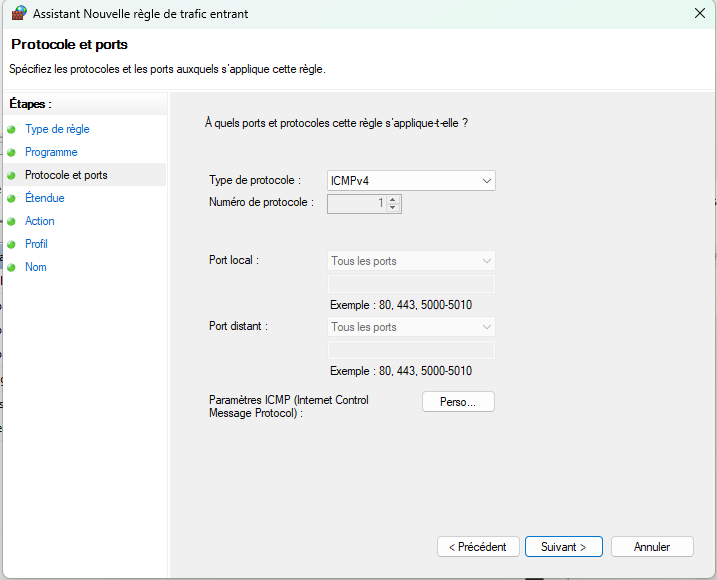
Dans la boîte de dialogue qui s'affiche, sélectionnez "Personnalisée" et cliquez sur "Suivant".



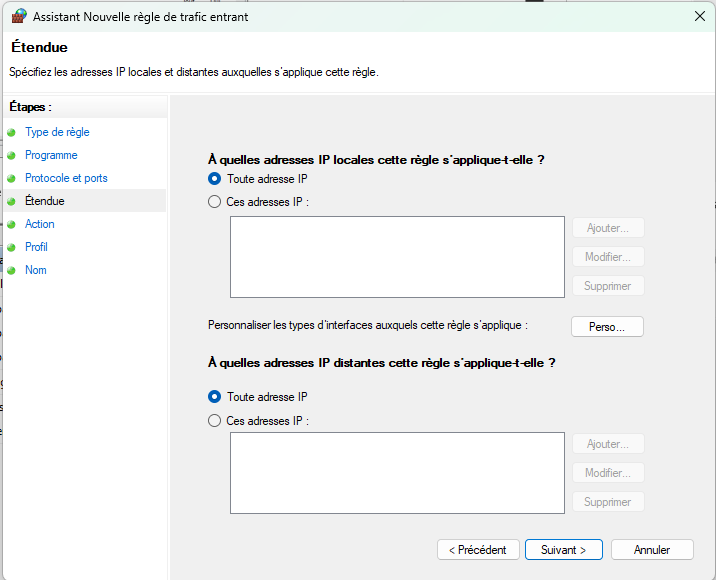
Sélectionnez « tous les programme » pour bloquer les connexions sortantes.



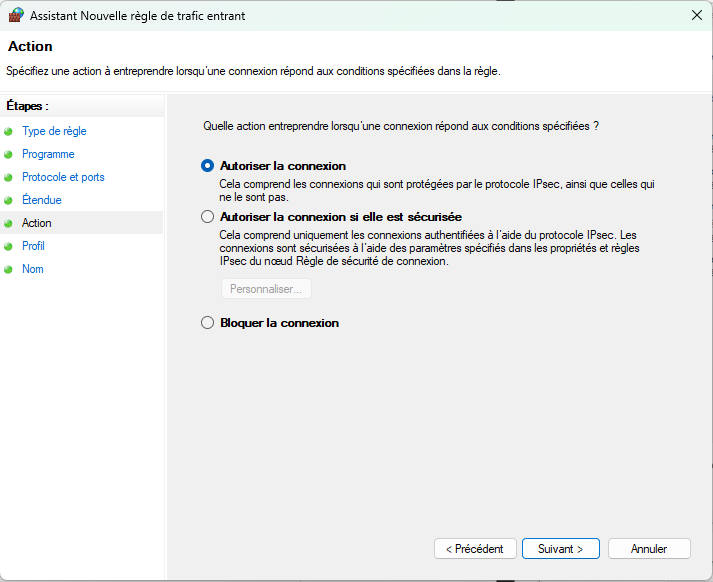
Dans la boîte de dialogue "Protocoles et ports", sélectionnez "ICMPV4" et cliquez sur "Suivant".



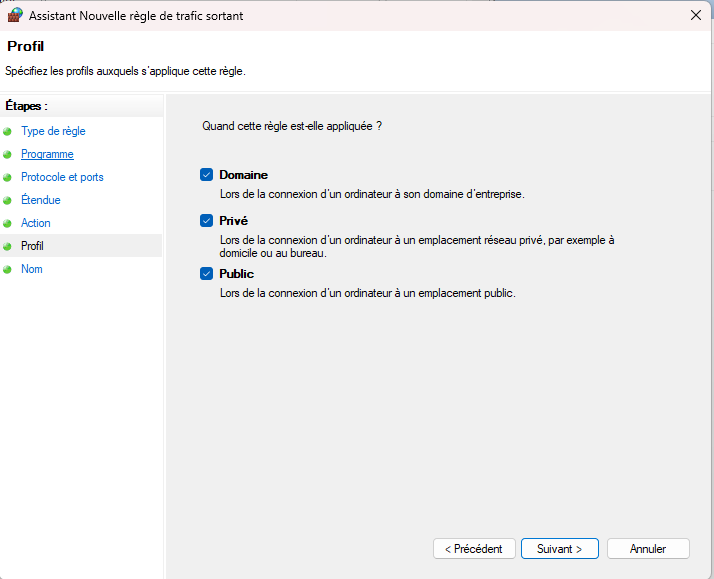
Dans la boîte de dialogue "Etendue", cliquez sur "Suivant".

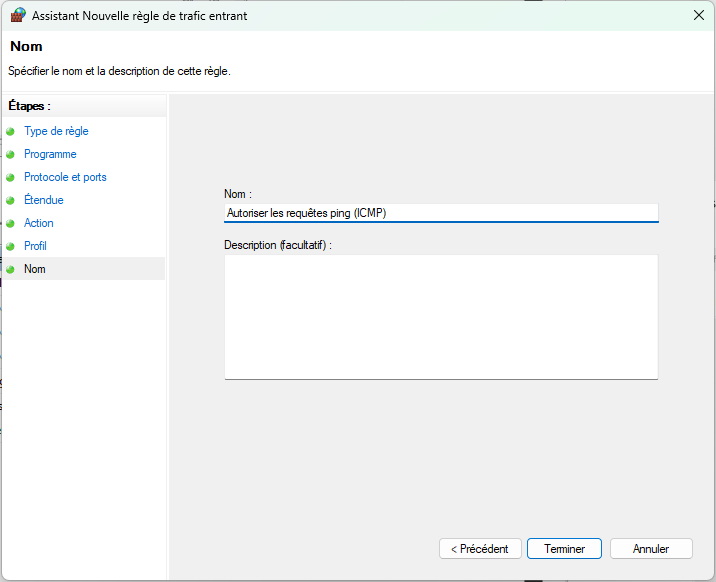


Sélectionnez "Autoriser la connexion" et cliquez sur "Suivant".



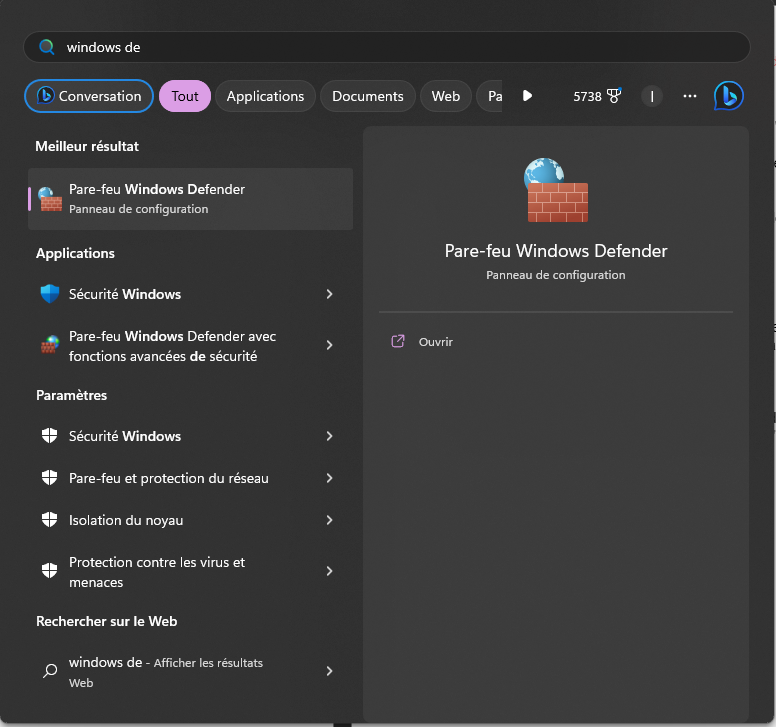
Cochez les cases correspondant aux profils de réseau pour lesquels vous voulez bloquer les connexions sortantes, puis cliquez sur "Suivant".

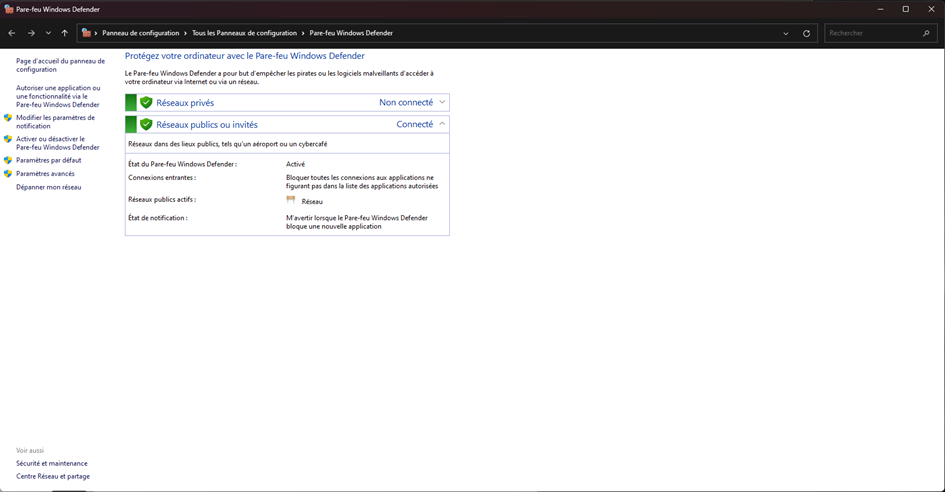


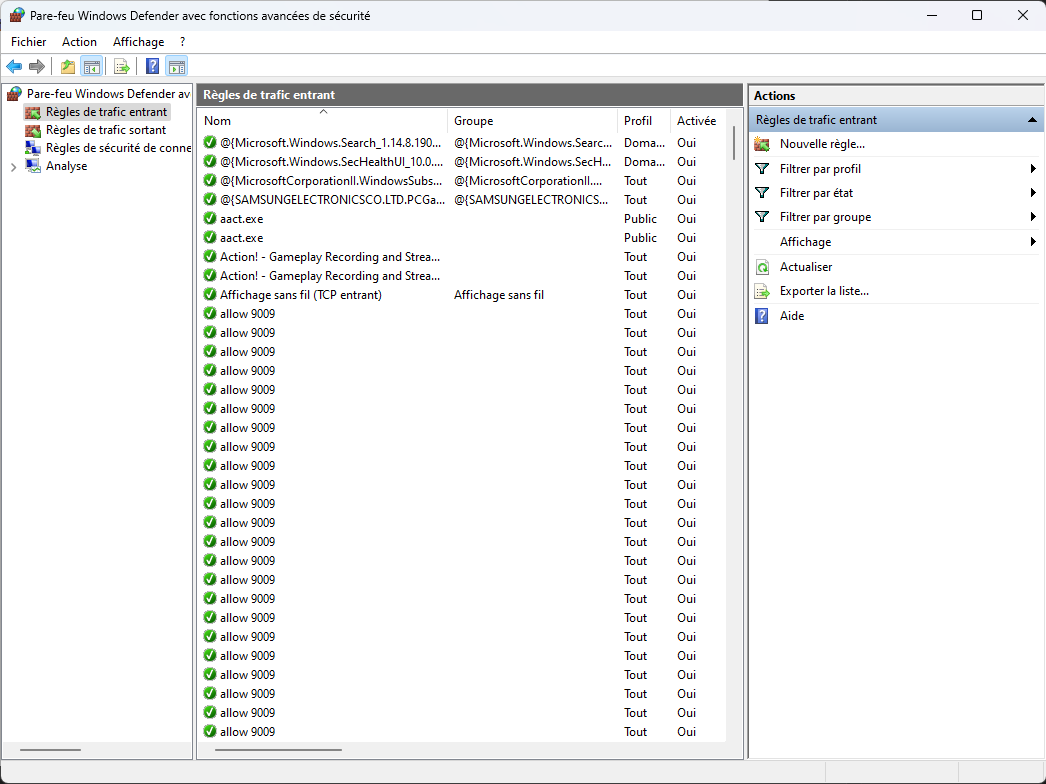
Donnez un nom à la règle, par exemple "Autoriser les requêtes ping (ICMP)", puis cliquez sur "Terminer".

Le poste doit permettre la prise en main bureau distant depuis un poste de votre réseau.

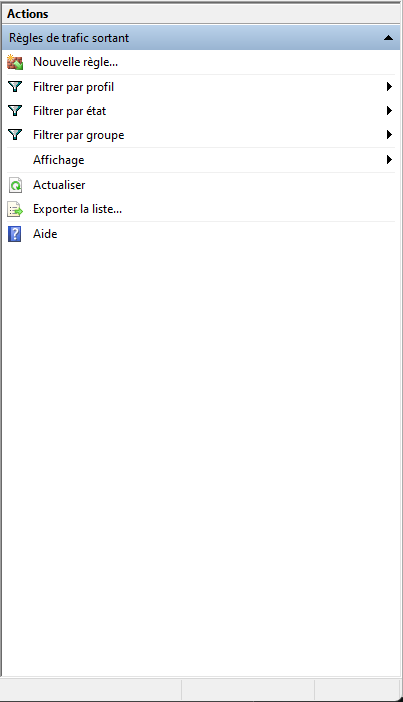
Voici comment paramétrer Windows Defender pour permettre la prise en main bureau à distance depuis un poste de votre réseau en filtrant les connexions sortantes :

Tout d'abord, ouvrez Windows Defender en cliquant sur le bouton "Démarrer" de Windows, en tapant "Windows Defender" dans la barre de recherche et en sélectionnant l'application "Windows Defender Firewall avec des fonctions avancées de sécurité".

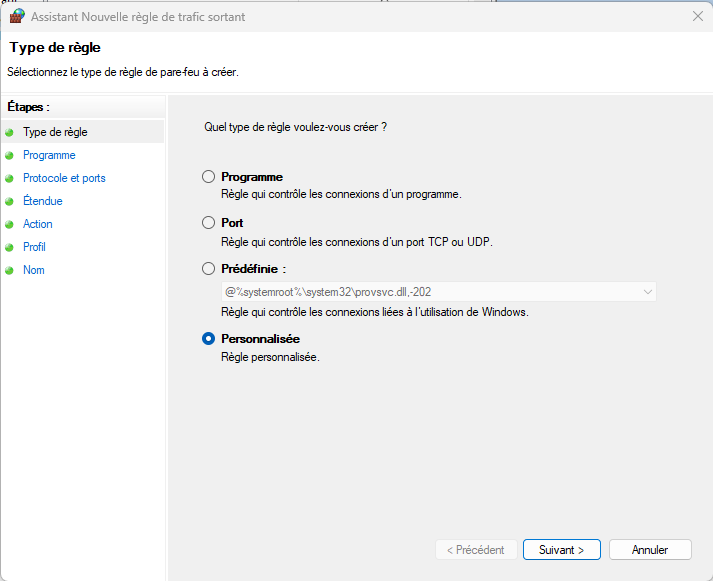
Dans la fenêtre de Windows Defender, cliquez sur "Paramètres avancés" dans le volet de gauche.

Dans la fenêtre de Windows Defender, cliquez sur "Règles de trafic sortant" dans le volet de gauche.

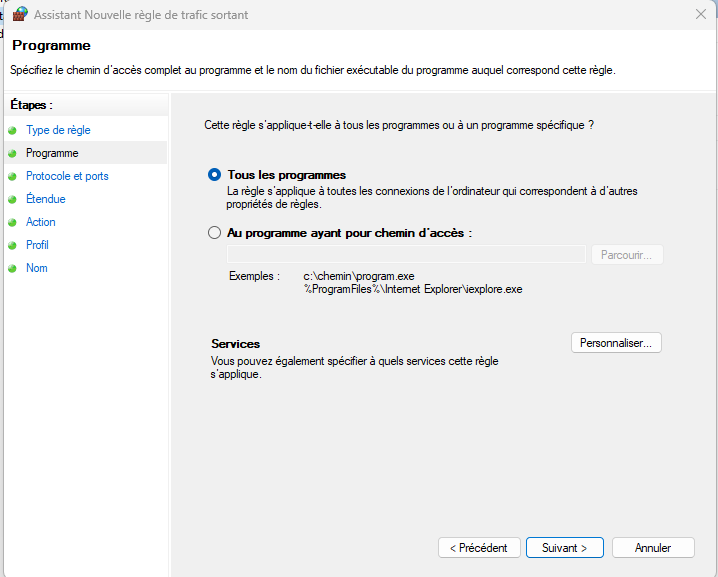
Cliquez sur "Nouvelle règle..." dans le volet de droite.



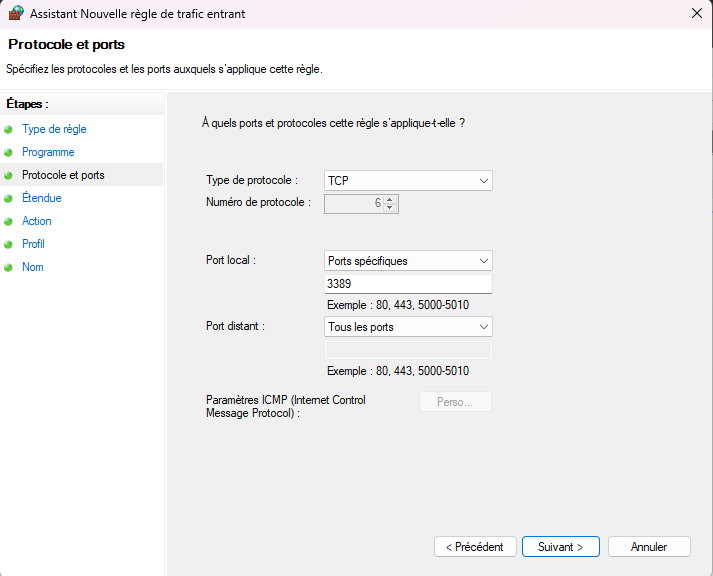
Dans la boîte de dialogue qui s'affiche, sélectionnez "Personnalisée" et cliquez sur "Suivant".



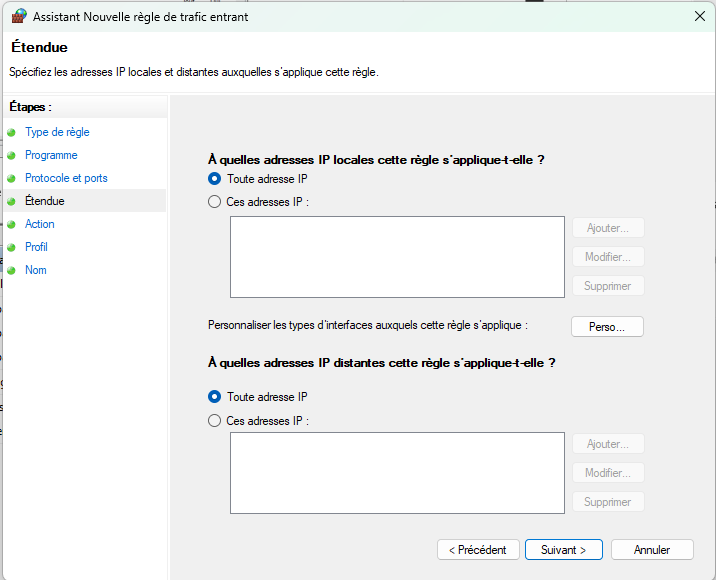
Sélectionnez « tous les programme » pour bloquer les connexions sortantes.



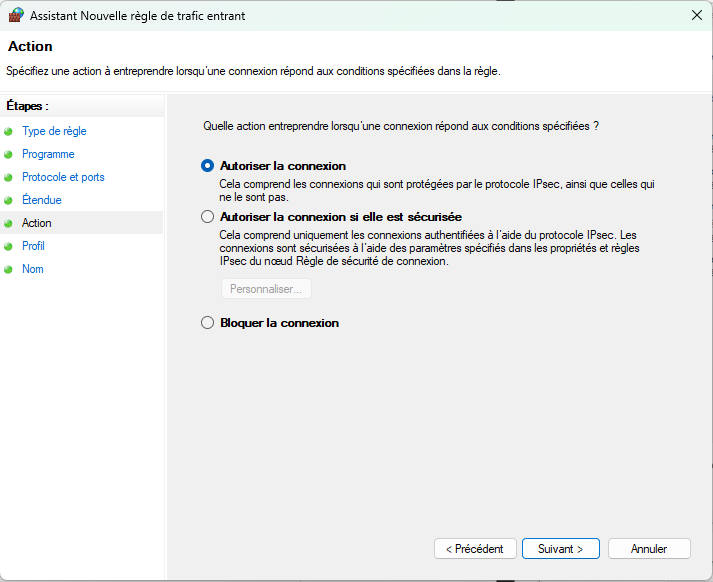
Dans la boîte de dialogue "Protocoles et ports", Sélectionnez "TCP" et cochez la case "Spécifique" pour les ports locaux.Entrez "3389" dans le champ "Ports locaux spécifiques" pour autoriser la prise en main bureau à distance sur le port TCP 3389.Cliquez sur "Suivant".



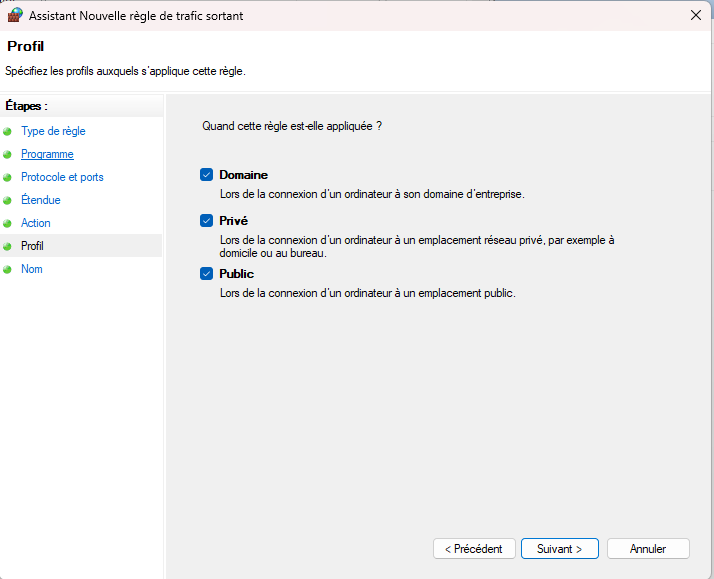
Dans la boîte de dialogue "Etendue", cliquez sur "Suivant".

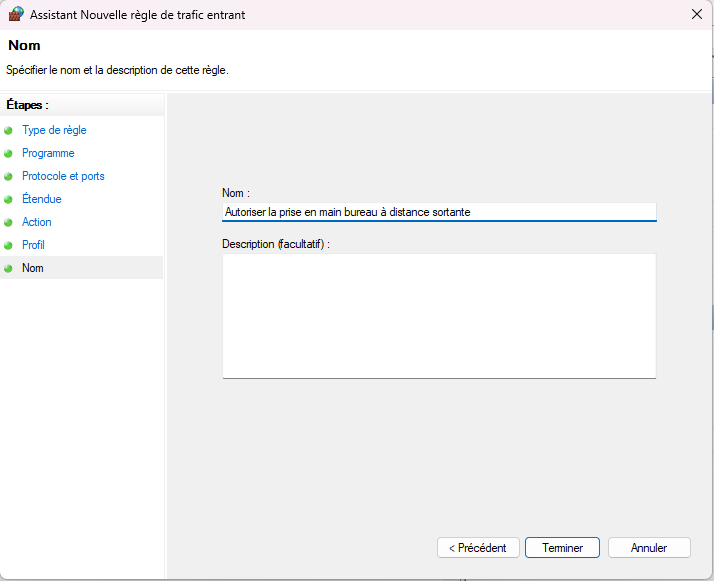


Sélectionnez "Autoriser la connexion" et cliquez sur "Suivant".



Cochez les cases correspondant aux profils de réseau pour lesquels vous voulez bloquer les connexions sortantes, puis cliquez sur "Suivant".

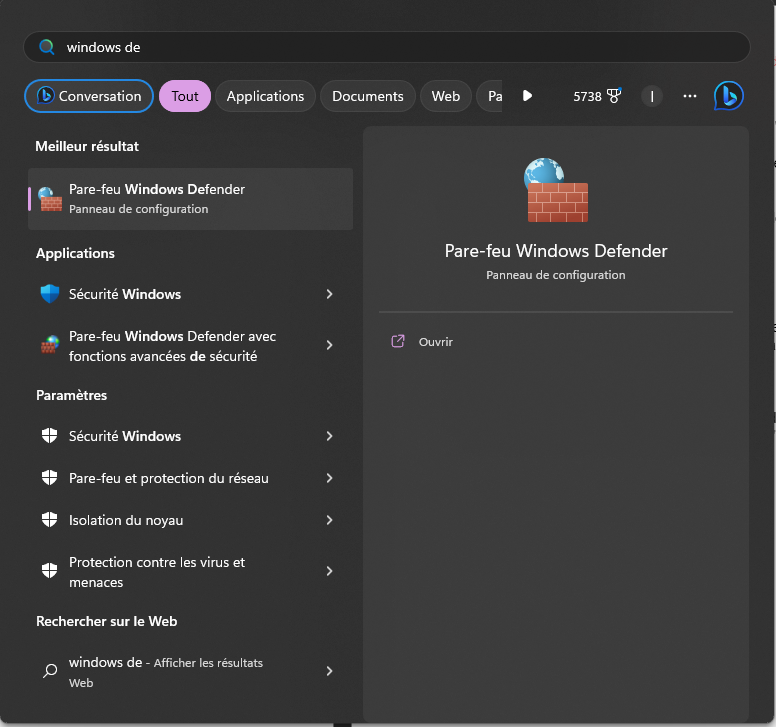


Dans la boîte de dialogue "Nom", donnez un nom à la règle "Autoriser la prise en main bureau à distance sortante", puis cliquez sur "Terminer".

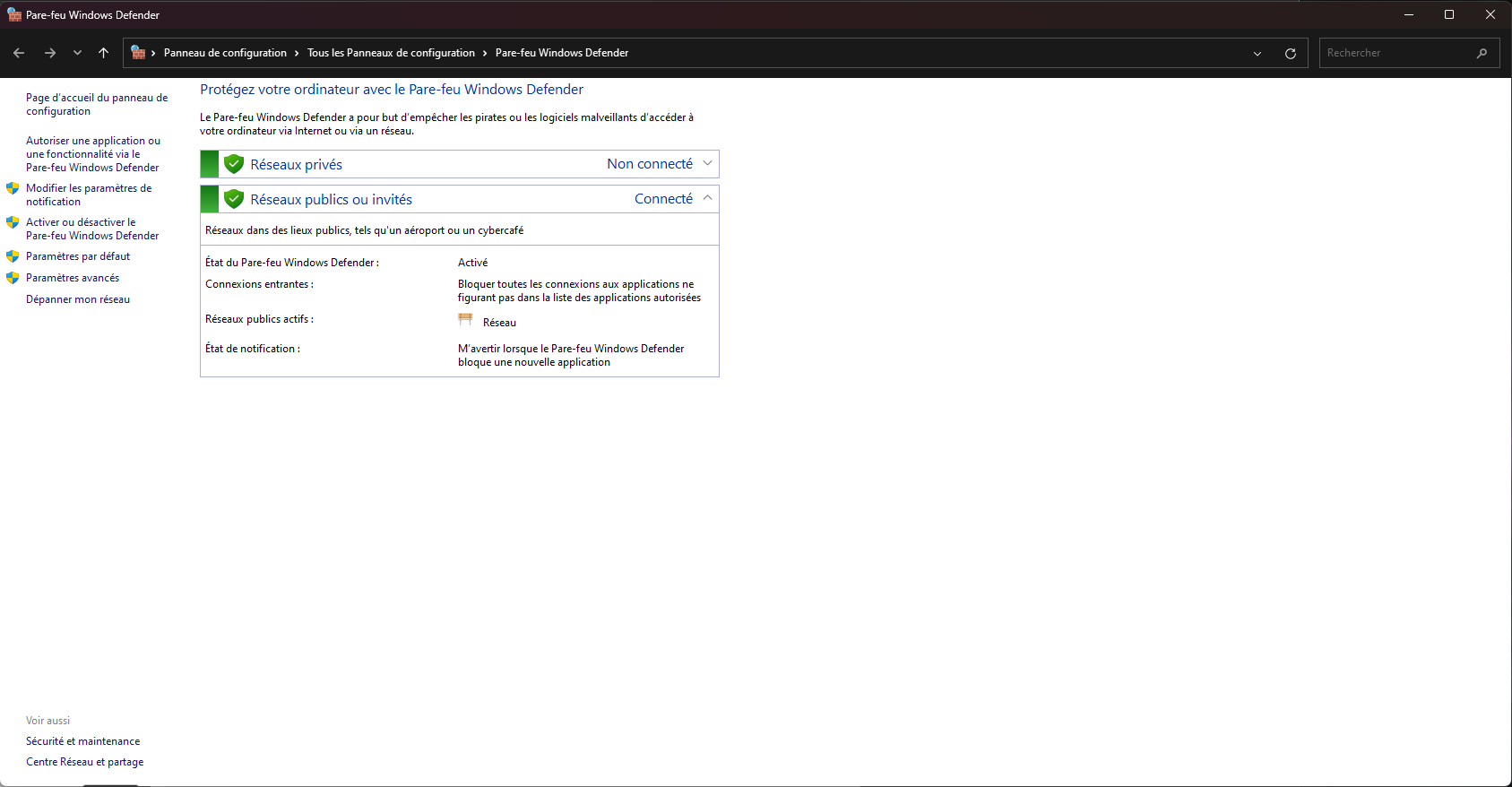
Toutes les autres connexions entrantes sont bloquées

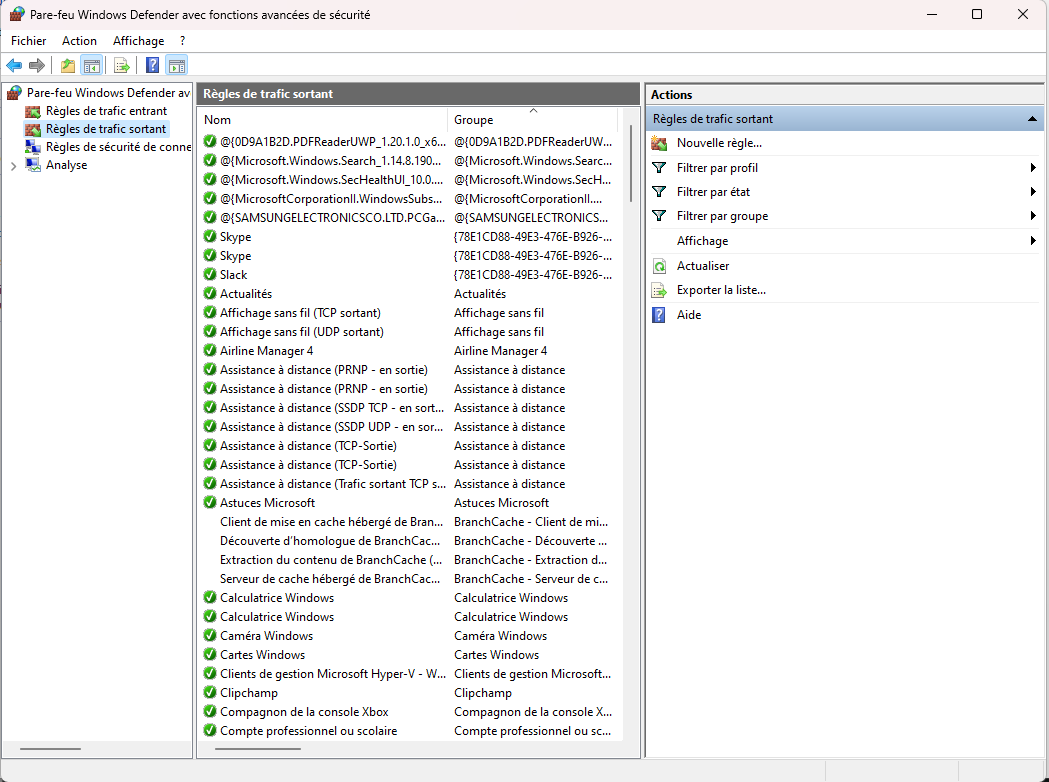
Voici comment paramétrer Windows Defender pour bloquer toutes les connexions entrantes, sauf celles spécifiées

Tout d'abord, ouvrez Windows Defender en cliquant sur le bouton "Démarrer" de Windows, en tapant "Windows Defender" dans la barre de recherche et en sélectionnant l'application "Windows Defender Firewall avec des fonctions avancées de sécurité".

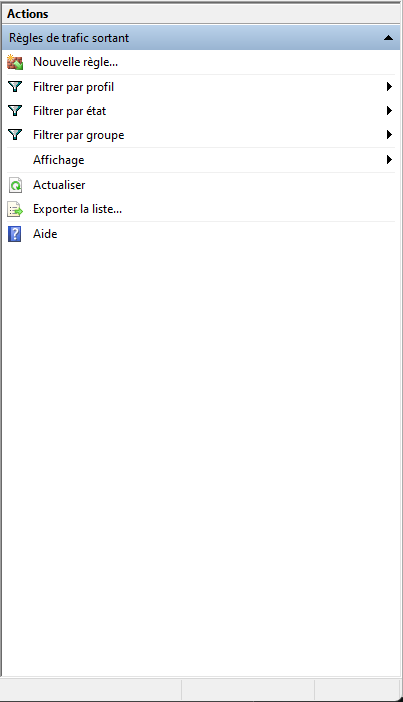


Dans la fenêtre de Windows Defender, cliquez sur "Paramètres avancés" dans le volet de gauche.

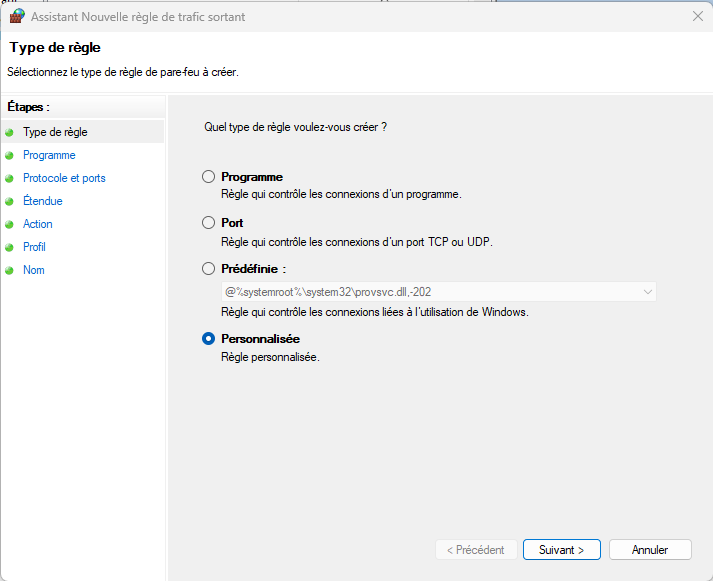


Dans la fenêtre de Windows Defender, cliquez sur "Règles de trafic sortant" dans le volet de gauche.

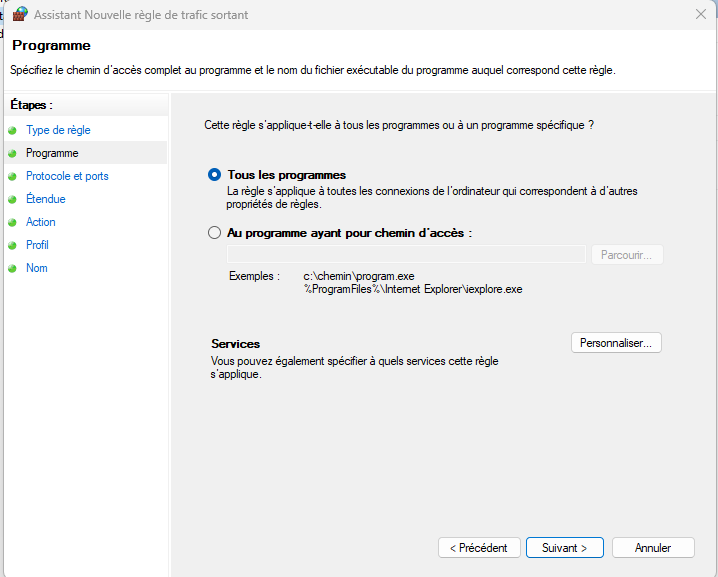
Cliquez sur "Nouvelle règle..." dans le volet de droite.



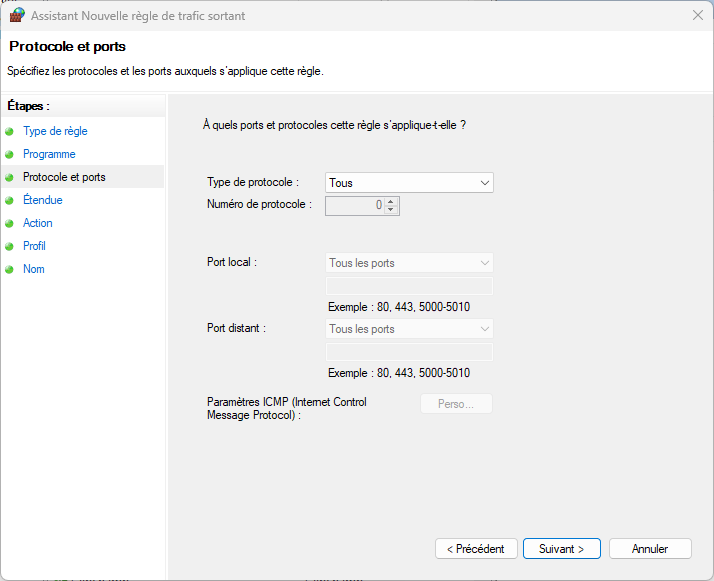
Dans la boîte de dialogue qui s'affiche, sélectionnez "Personnalisée" et cliquez sur "Suivant".



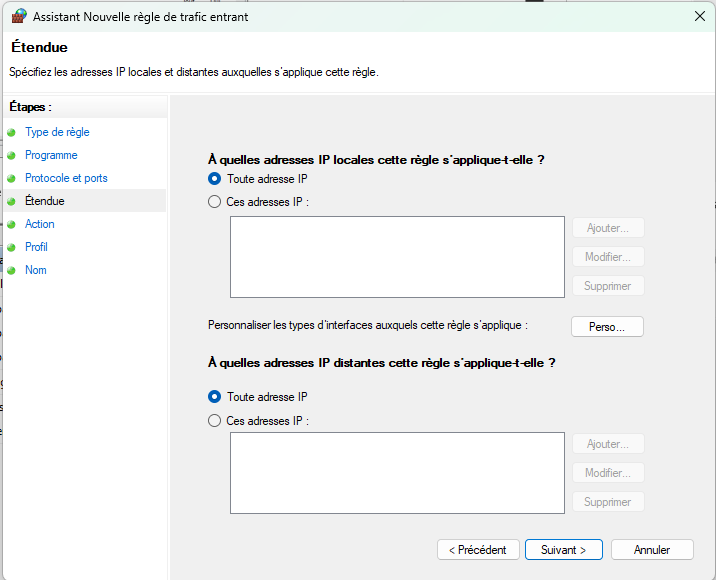
Sélectionnez « tous les programme » pour bloquer les connexions sortantes.



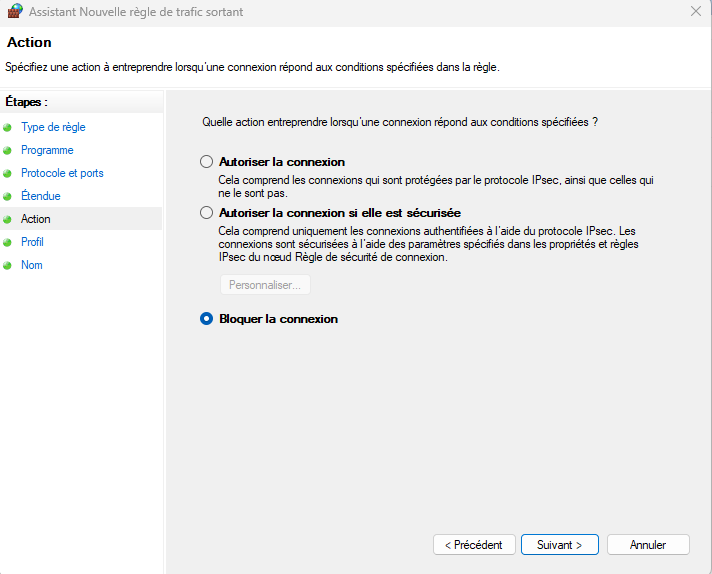
Dans la boîte de dialogue "Protocoles et ports", sélectionnez "Tous les ports" et cliquez sur "Suivant".



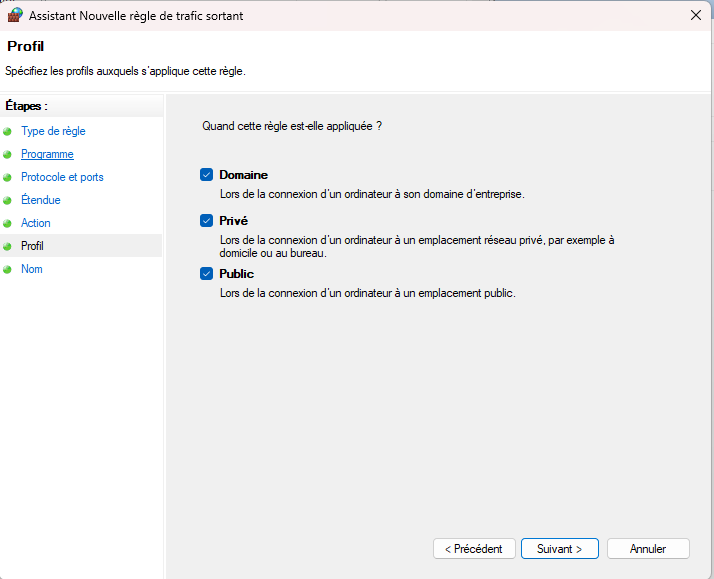
Dans la boîte de dialogue "Etendue", cliquez sur "Suivant".



Sélectionnez "Bloquer la connexion" et cliquez sur "Suivant".



Cochez les cases correspondant aux profils de réseau pour lesquels vous voulez bloquer les connexions sortantes, puis cliquez sur "Suivant".



Donnez un nom à la règle, par exemple "Blocage des connexions entrantes sauf spécifiées", puis cliquez sur "Terminer".

