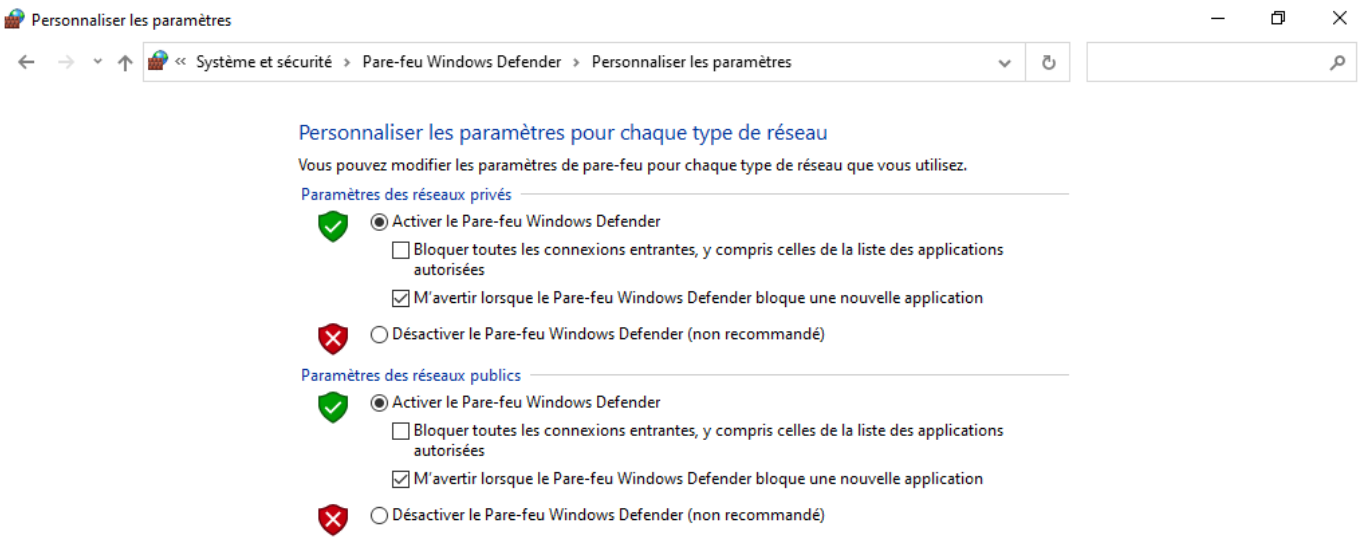
Firewall Windows

Sommaire:

Activer le pare-feu

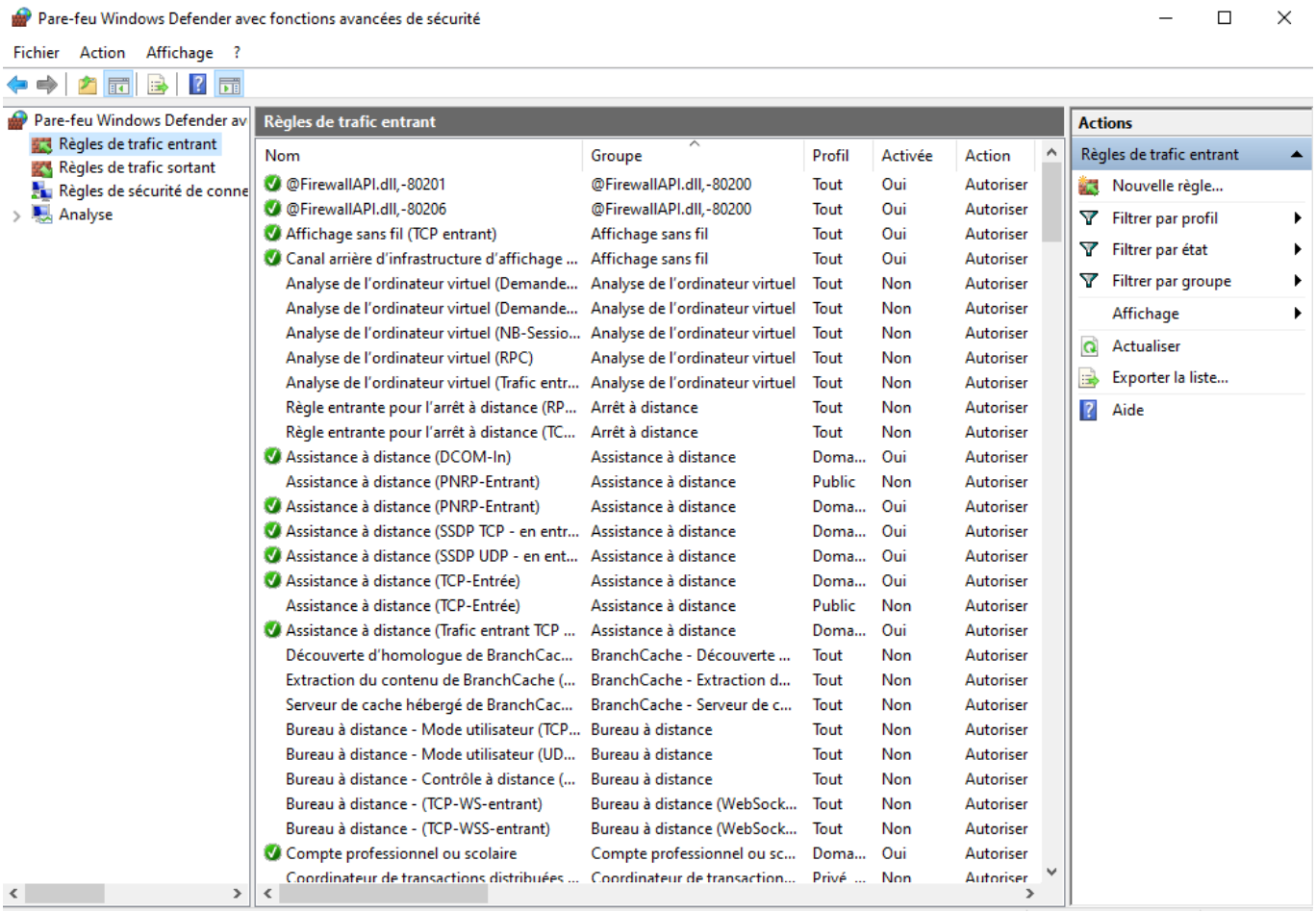
Pour activer le pare-feu Windows il faut d'abord accéder au *Pare-feu Windows Defender* > *Activer ou désactiver le Pare-feu Windows Defender* depuis la barre de recherche.



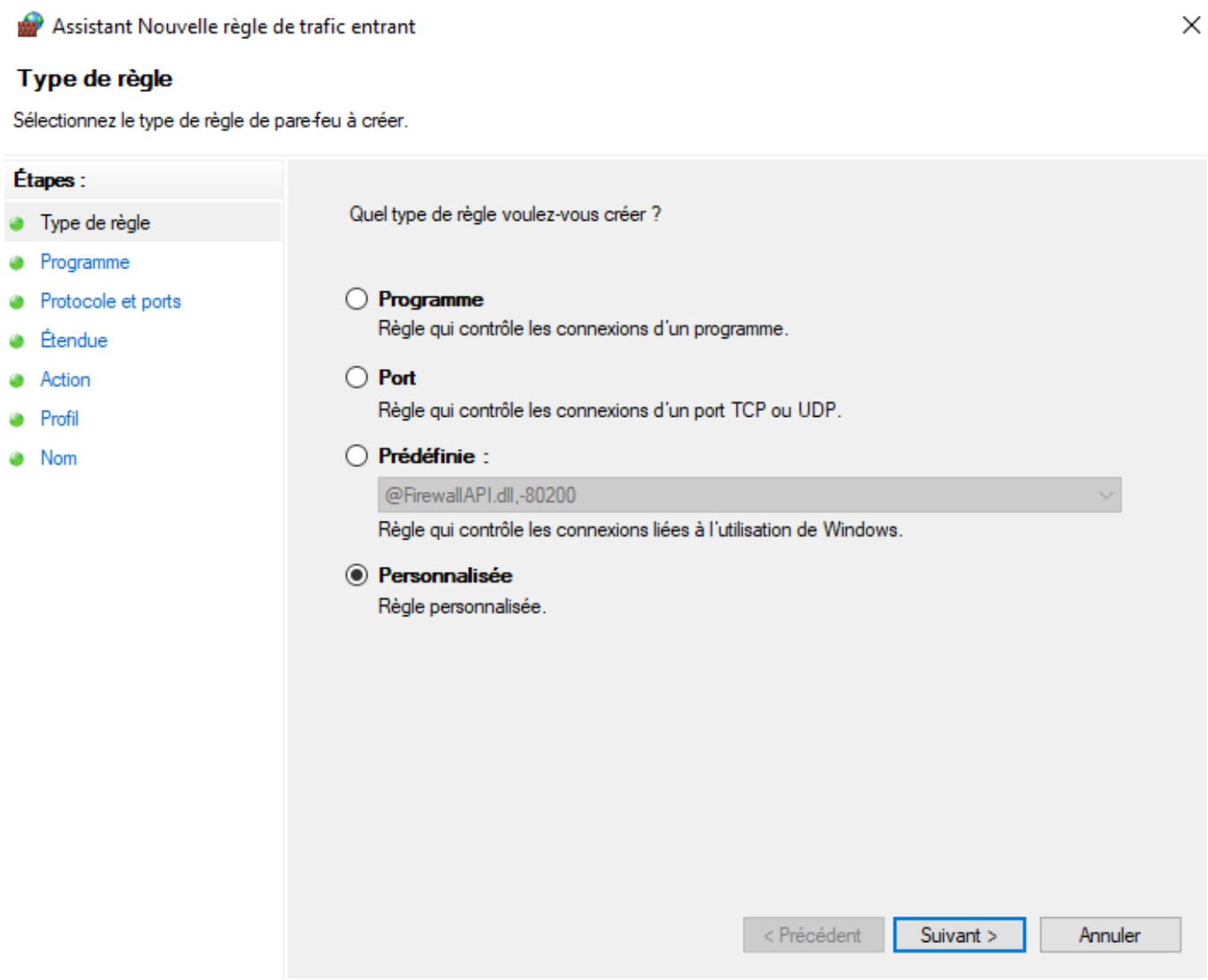
Il faut appuyer sur activer sur les différents réseaux qui nous intéressent.

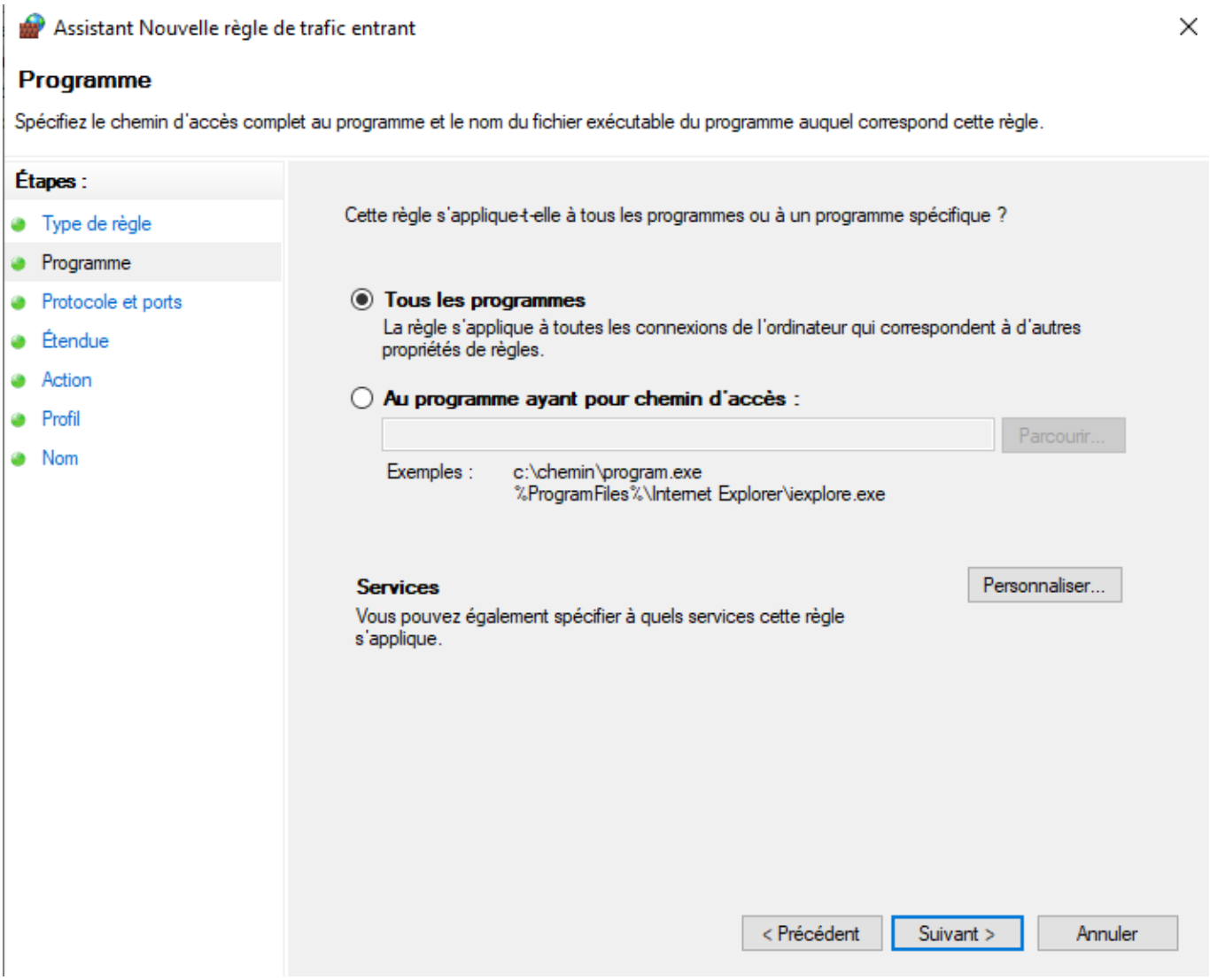
Créer une règle

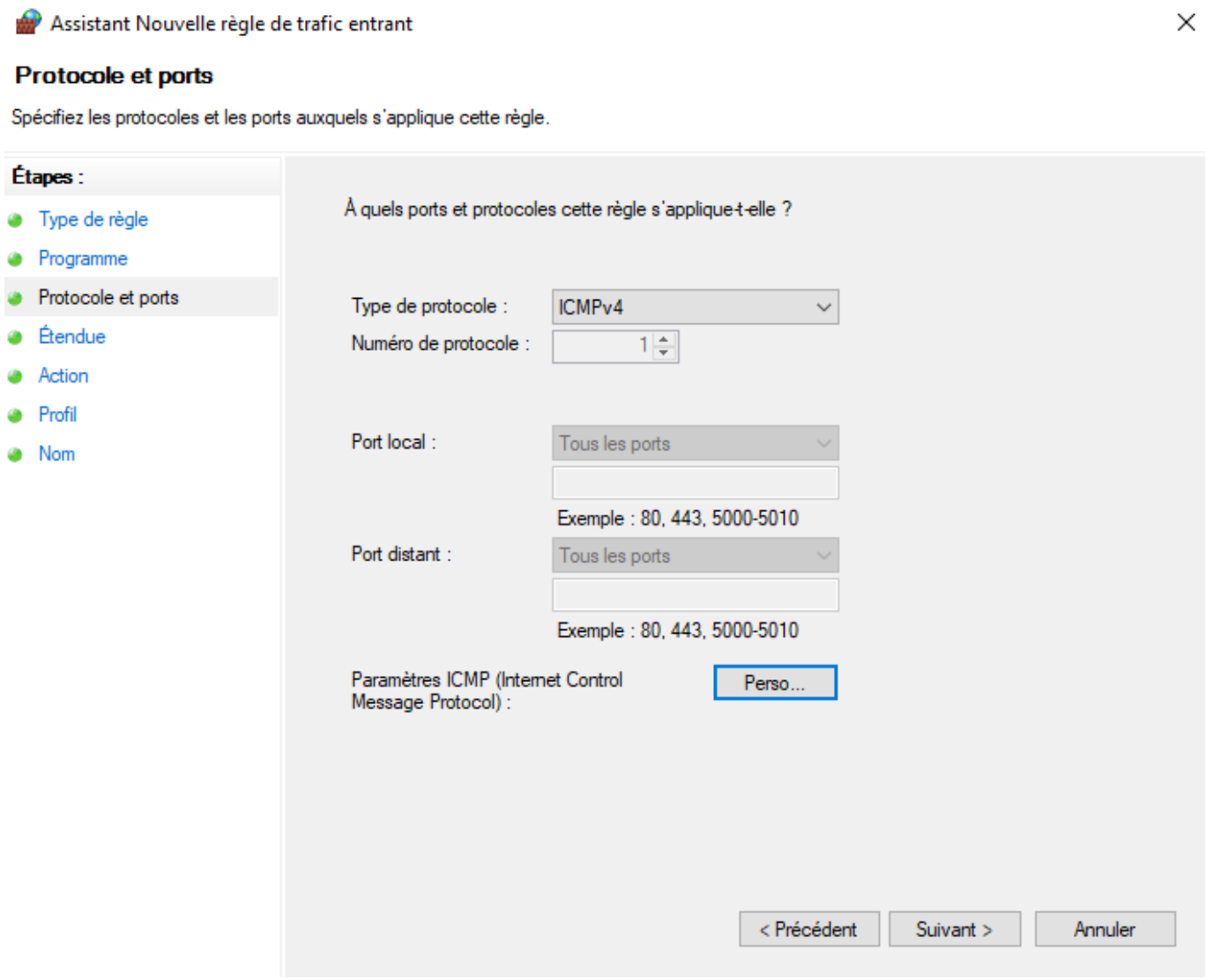
Pour créer une règle il faut tout d'abord accéder à *Pare-feu Windows Defender* > *Paramètres avancés*.
Il faut ensuite clicker sur l'option *Règles de trafic entrant* puis sur *Nouvelle règle*.



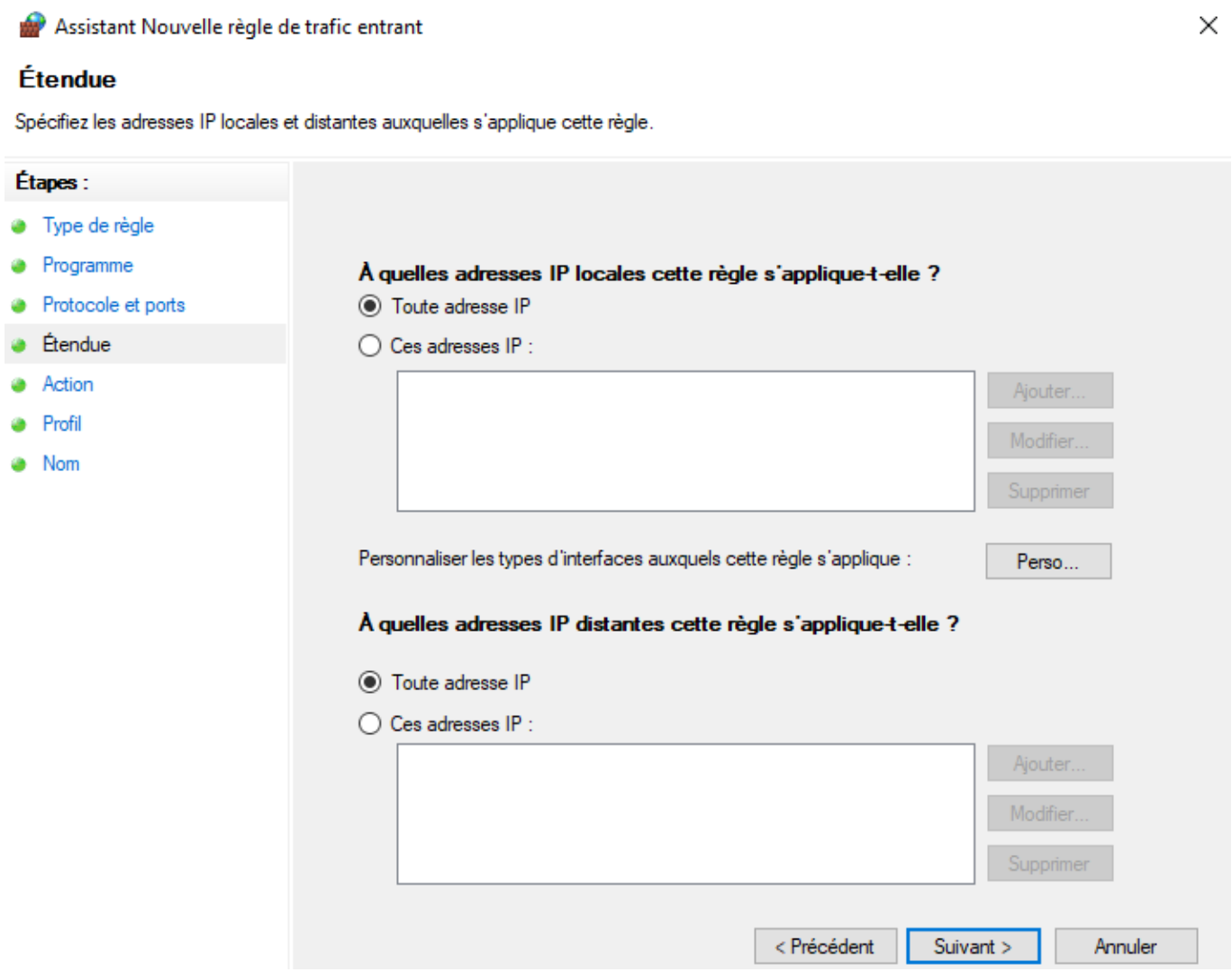
Ensuite il faut suivre les images suivantes:


Assistant Nouvelle règle de trafic entrant
Type de règle
Sélectionnez le type de règle de pare-feu à créer.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Quel type de règle voulez-vous créer ?
Programme
Règle qui contrôle les connexions d'un programme.
Port
Règle qui contrôle les connexions d'un port TCP ou UDP.
Prédéfinie :
@FirewallAPI.dll,-80200
Règle qui contrôle les connexions liées à l'utilisation de Windows.
Personnalisée
Règle personnalisée.
< Précédent
Suivant >
Annuler

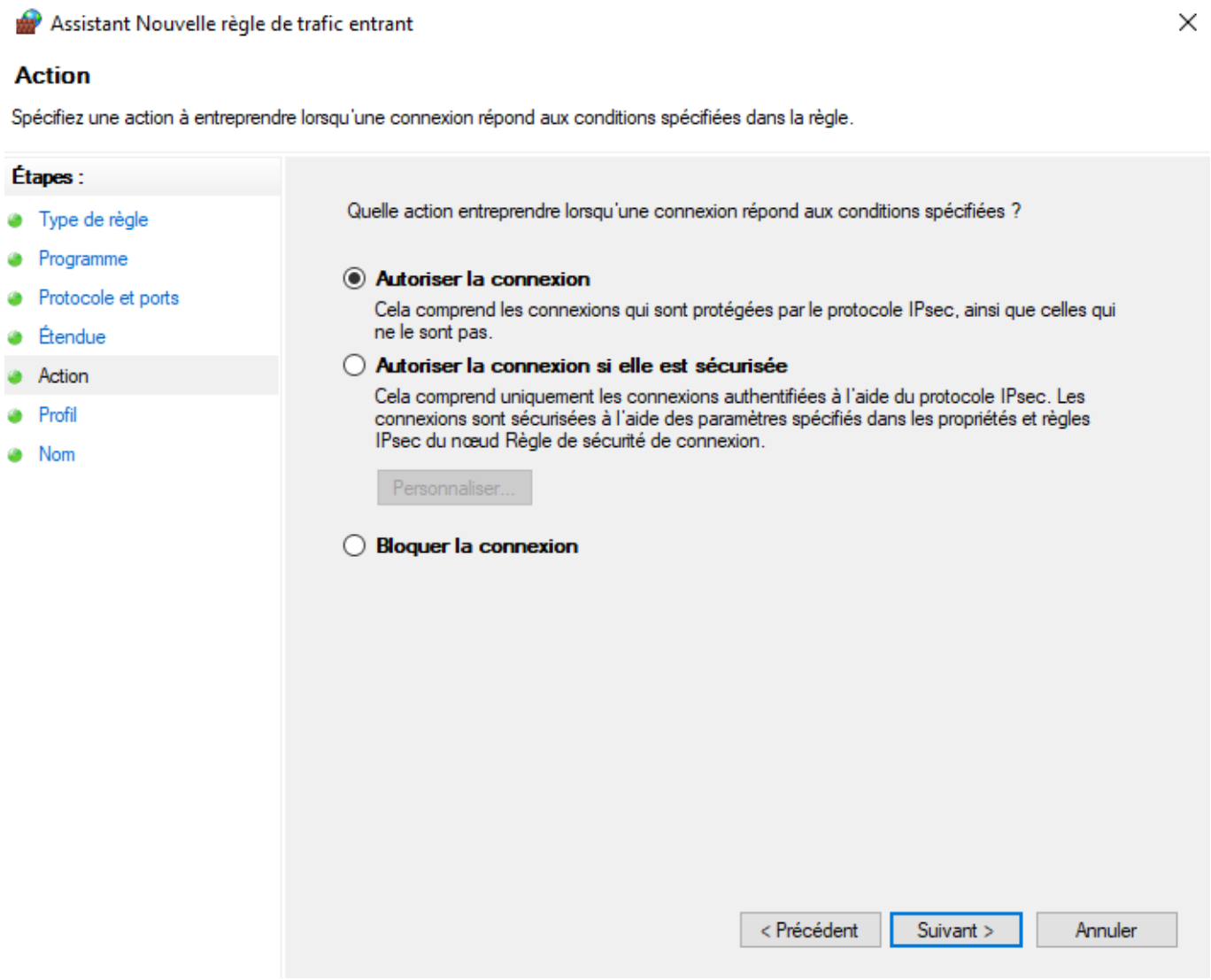

Assistant Nouvelle règle de trafic entrant
Programme
Spécifiez le chemin d'accès complet au programme et le nom du fichier exécutable du programme auquel correspond cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Cette règle s'applique-t-elle à tous les programmes ou à un programme spécifique ?
Tous les programmes
La règle s'applique à toutes les connexions de l'ordinateur qui correspondent à d'autres propriétés de règles.
Au programme ayant pour chemin d'accès :
Parcourir...
Exemples : c:\chemin\program.exe
%ProgramFiles%\Internet Explorer\iexplore.exe
Services
Vous pouvez également spécifier à quels services cette règle s'applique.
Personnaliser...
< Précédent
Suivant >
Annuler



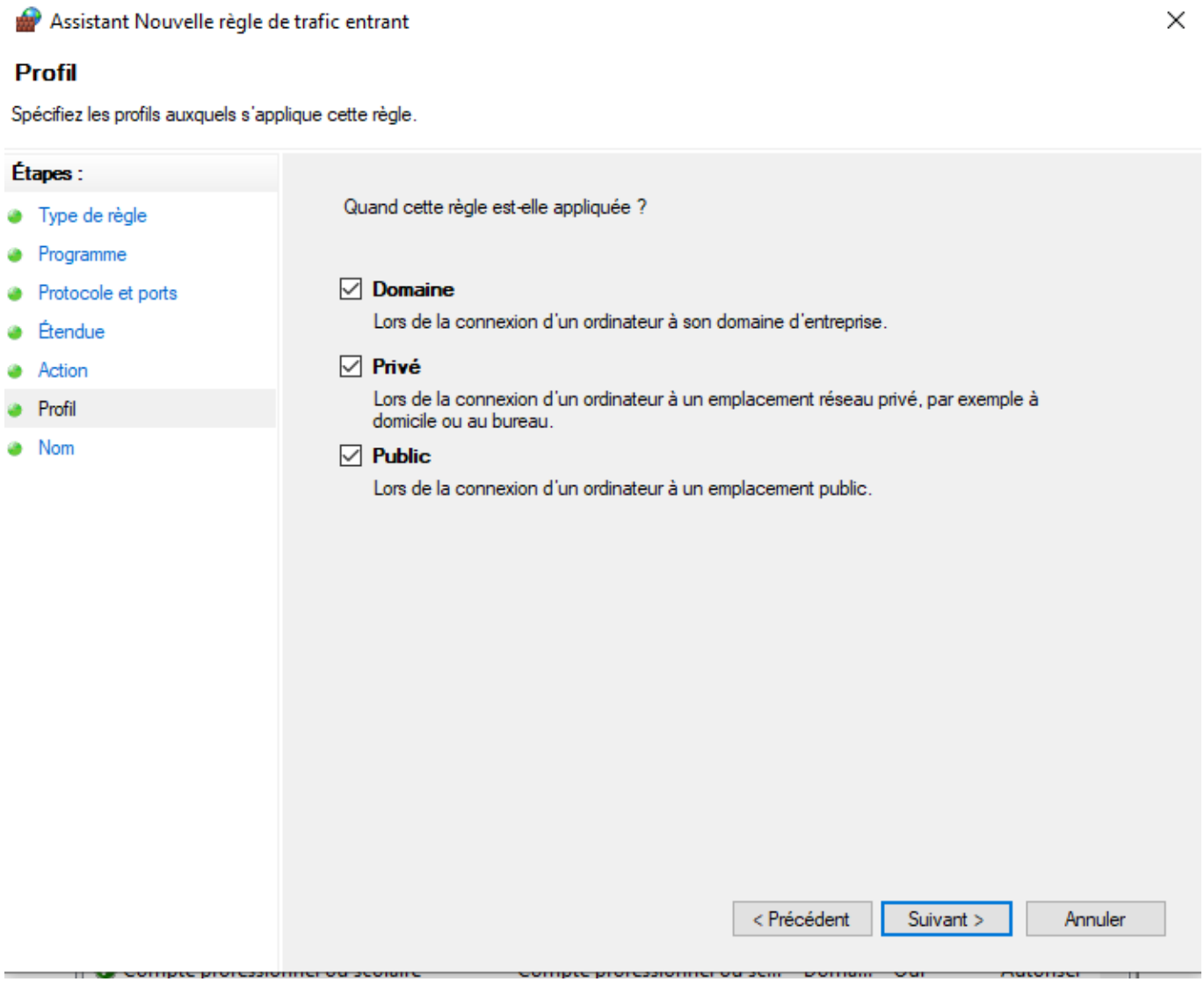
Il faudra choisir les protocoles et les ports qui nous conviennent.



Ici on peut choisir si on veut limiter la règle à certaines IP que l'on précise.



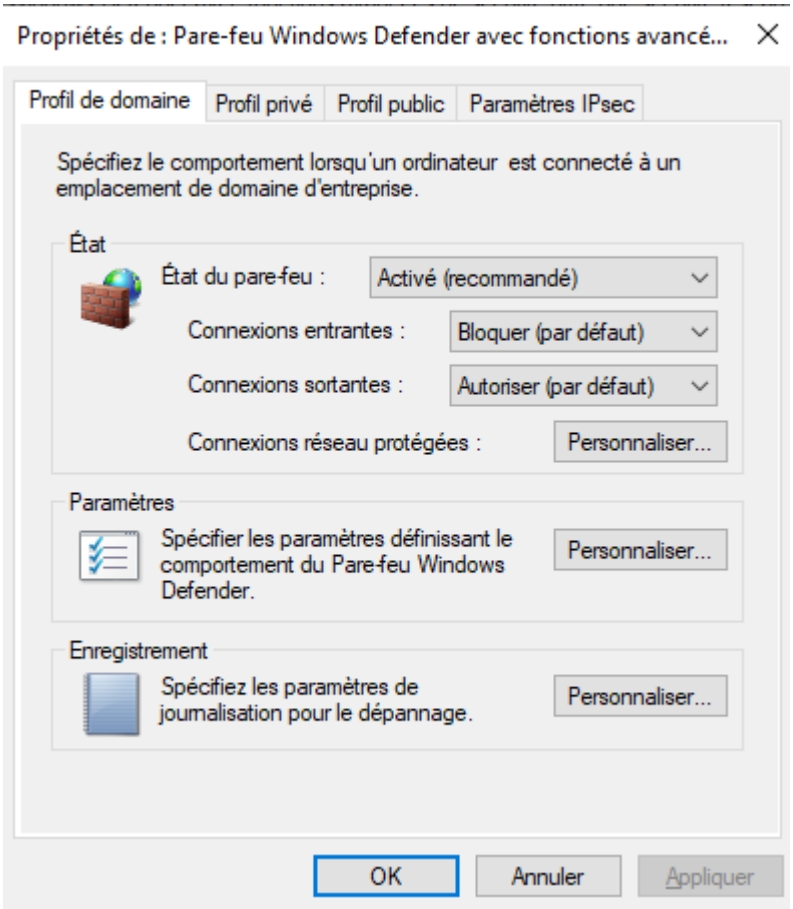
On choisit si on veut autoriser ou bloquer l'action.

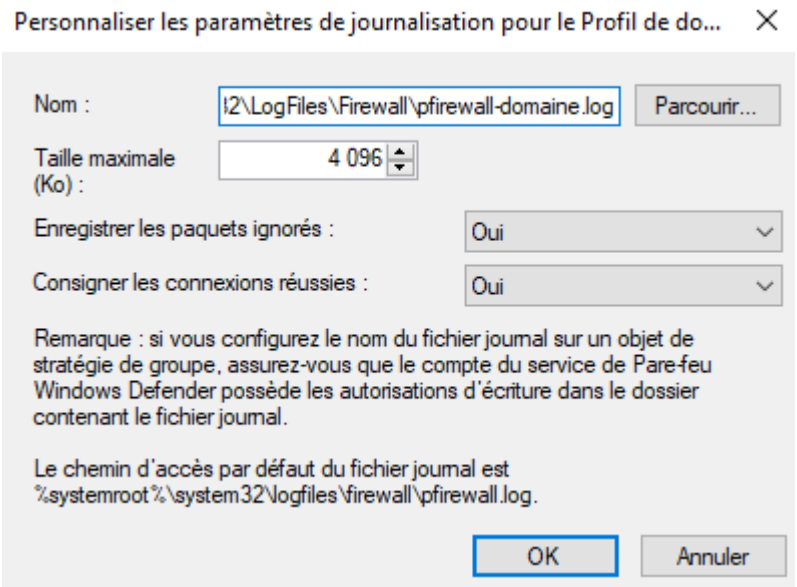


On choisit les profils auquels cette règle est appliquée.

Journaliser/LOG

La journalisation va nous permettre d'enregistrer toutes les actions qui sont faites au niveau de notre carte réseau.
Pour commencer l'enregistrement on va tout d'abord acceder aux propriétes du pare-feu depuis les options avancés.





Il va falloir configurer chaque profil pour enregistrer TOUTES les actions.

Exporter le LOG (CSV)

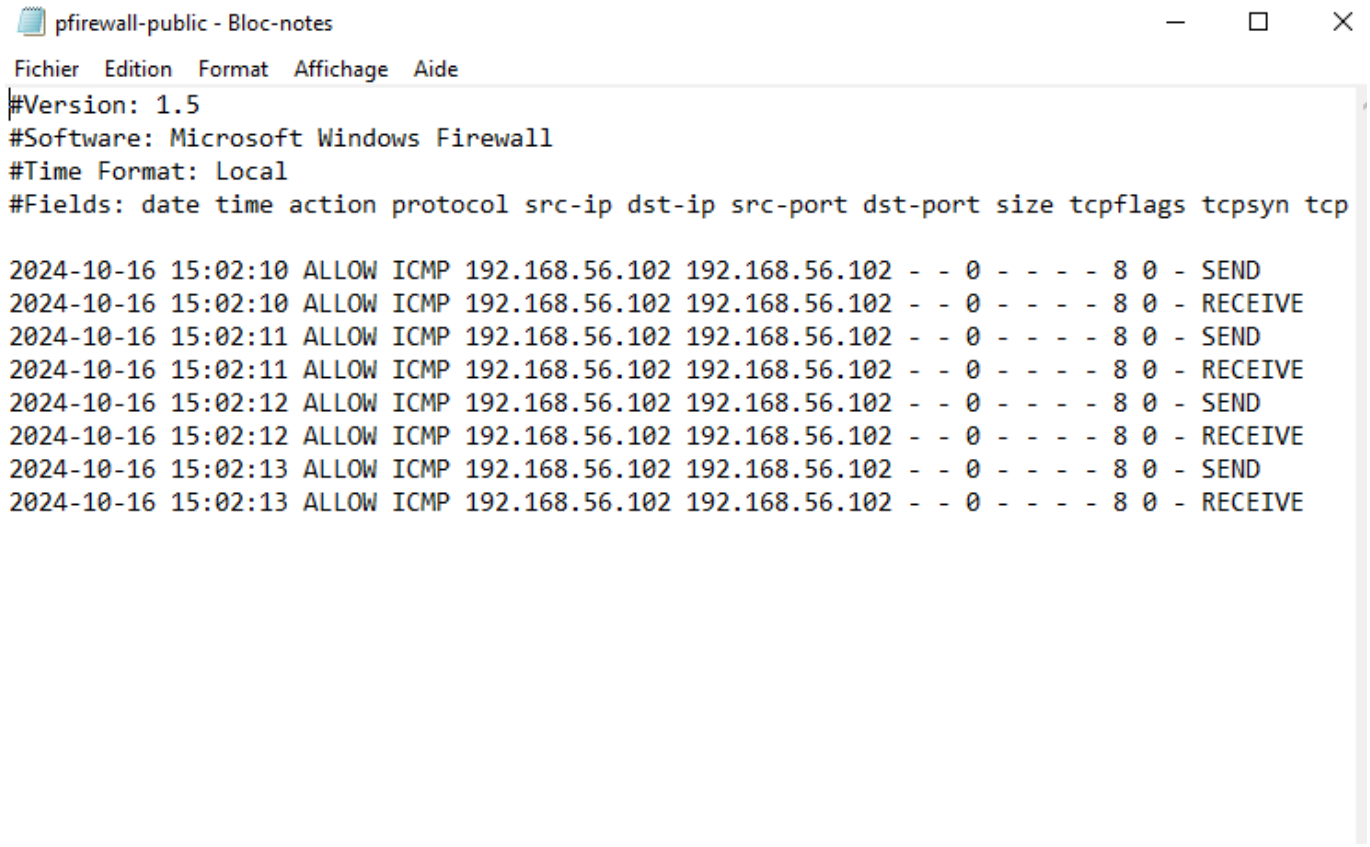
Tout d'abord il faut accéder aux logs. Pour faire cela il va falloir accéder au dossier d'enregistrement qui est paramétré sur le point d'avant.

Par défaut on peut retrouver les logs sur le chemin suivant:

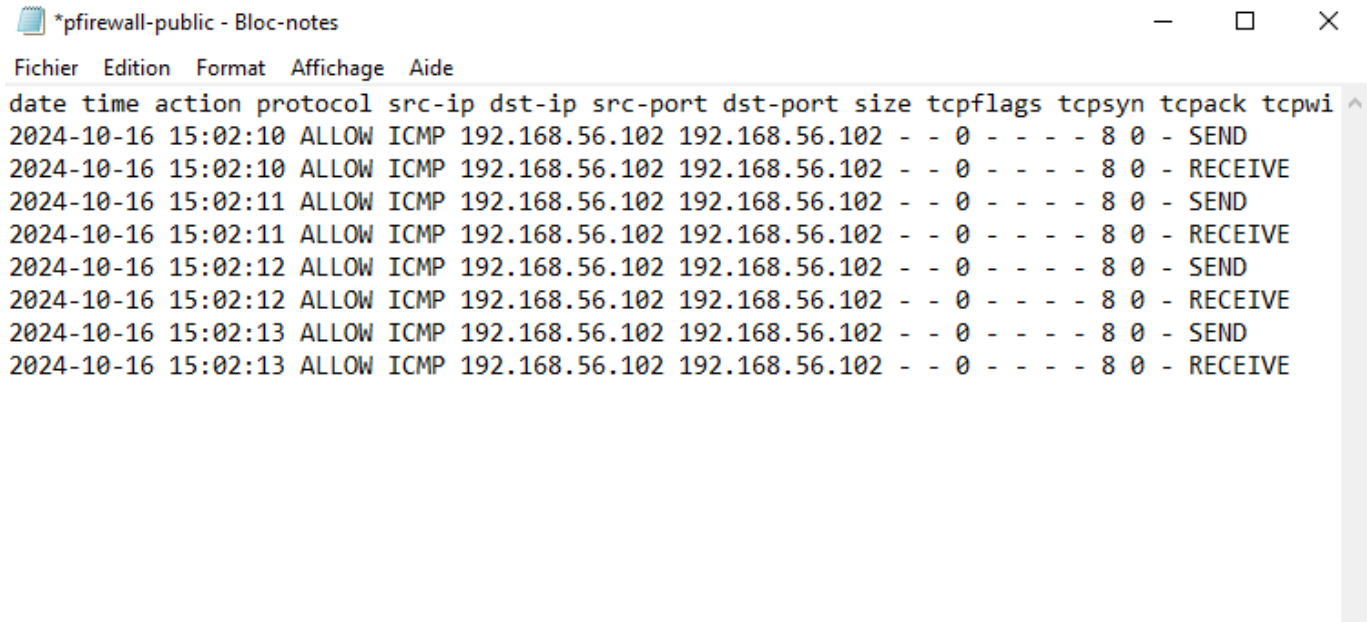
> %systemroot%\system32\LogFiles\Firewall\

On peut y accéder avec Win + R.

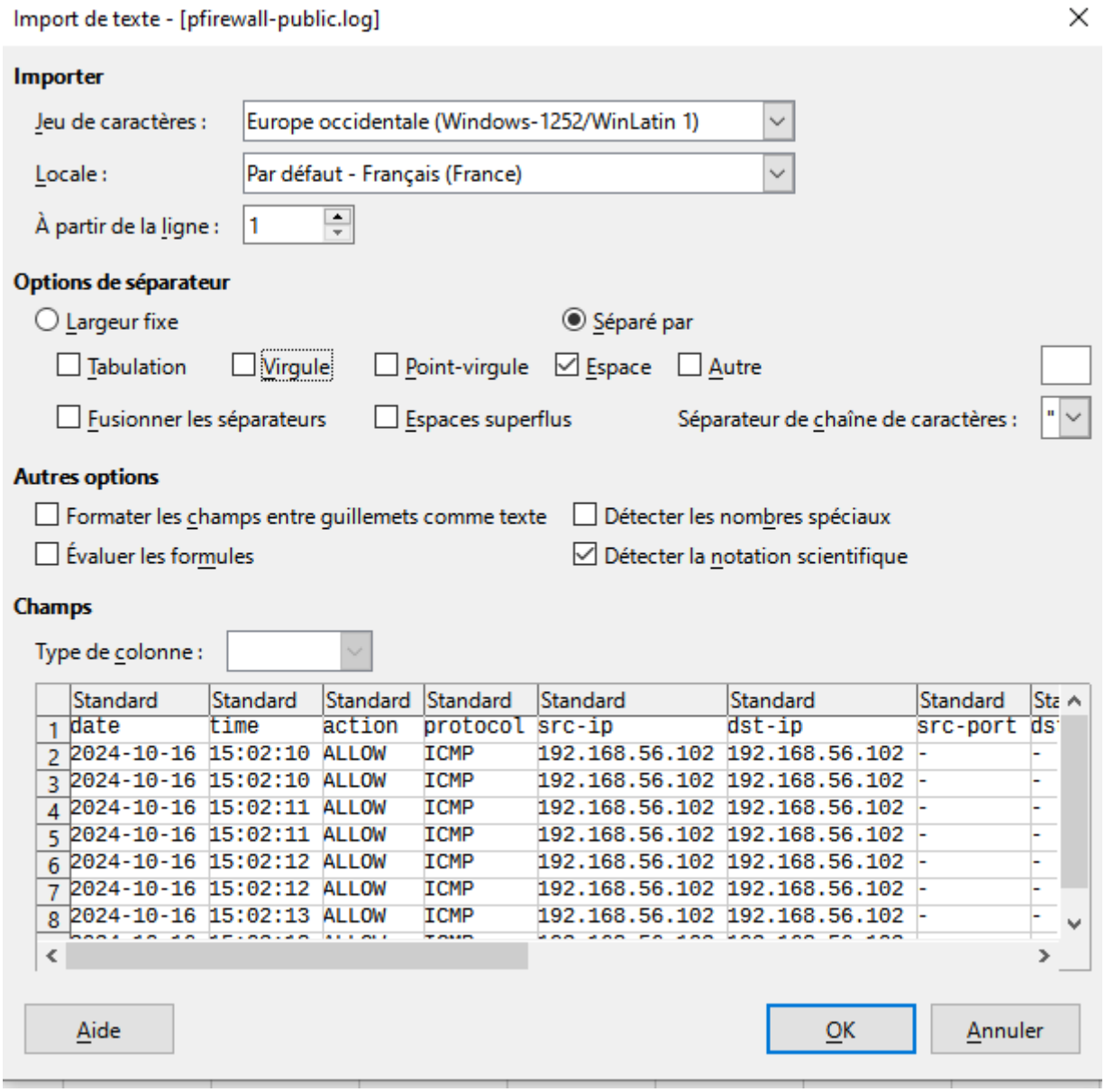
Si on ouvre directement le fichier LOG ça va être peu lisible, donc on va utiliser un logiciel comme excel pour le mettre en forme.



Tout d'abord il faut supprimer les commentaires qui suivent un signe "#". Le fichier devra ressembler à ça:



Enfin on va l'ouvrir avec le logiciel de notre choix soit en glissant le fichier ou en utilisant l'interface du logiciel pour ouvrir le fichier. Choisir l'option *Espace*.



	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Sta
1	date	time	action	protocol	src-ip	dst-ip	src-port	ds
2	2024-10-16	15:02:10	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-
3	2024-10-16	15:02:10	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-
4	2024-10-16	15:02:11	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-
5	2024-10-16	15:02:11	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-
6	2024-10-16	15:02:12	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-
7	2024-10-16	15:02:12	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-
8	2024-10-16	15:02:13	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-

date	time	action	protocol	src-ip	dst-ip	src-port	dst-port	size	tcpflags	tcpsyn	tcpack	tcpwin	icmptype	icmpcode	info	path
2024-10-16	15:02:10	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	SEND
2024-10-16	15:02:10	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	RECEIVE
2024-10-16	15:02:11	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	SEND
2024-10-16	15:02:11	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	RECEIVE
2024-10-16	15:02:12	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	SEND
2024-10-16	15:02:12	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	RECEIVE
2024-10-16	15:02:13	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	SEND
2024-10-16	15:02:13	ALLOW	ICMP	192.168.56.102	192.168.56.102	-	-	0	-	-	-	-	8	0	-	RECEIVE