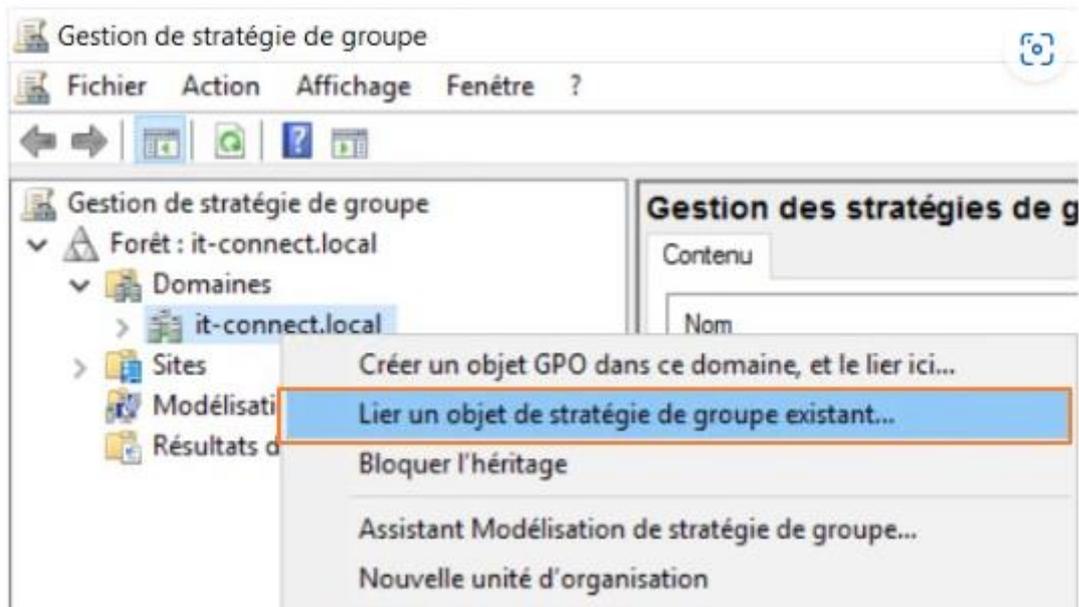


CONFIGURER LE PARE- FEU POUR SCCM

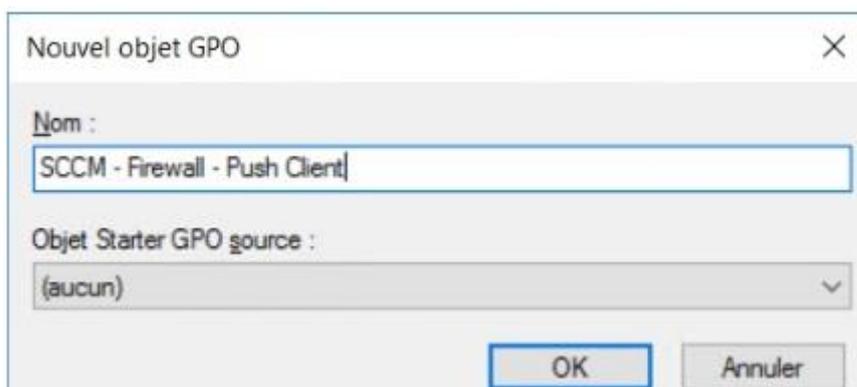
Mathis SZYDA

I. Création de la GPO avec les règles du firewall.

Sur votre contrôleur de domaine, au sein de la console gestion de stratégie de groupe, créez une nouvelle GPO :



Étant donné qu'elle va contenir les règles du pare-feu qui permettront de pusher le client sur les appareils gérés, on va la nommer "**SCCM - Firewall - Push Client**".



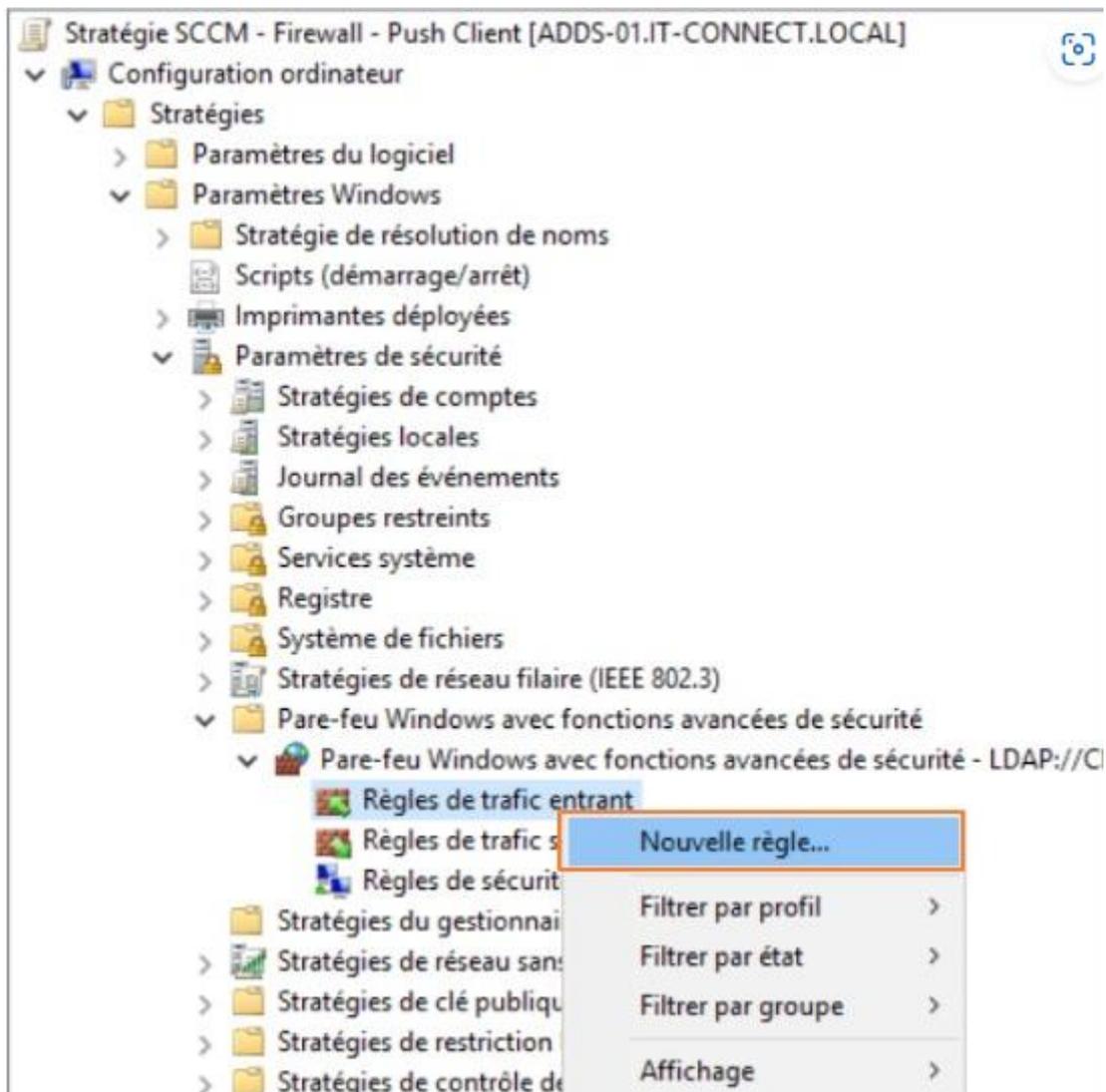
Éditez ensuite la GPO que l'on vient de créer : clic droit puis "Modifier".



A. Règle "Partage de fichiers et d'imprimantes"

Pour le paramétrage de règles de firewall, il faut accéder à : **Configuration ordinateur, Stratégie, Paramètres Windows, Paramètres de sécurité, Pare-feu Windows avec fonctions avancées de sécurité (x2).**

Sur "*Règles de trafic entrant*", effectuez un clic droit puis "*Nouvelle règle*".



Choisissez "*Prédéfinie*" comme type de règle et dans la liste sélectionnez "*Partage de fichiers et d'imprimantes*".

Assistant Nouvelle règle de trafic entrant ×

Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

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 :
Partage de fichiers et d'imprimantes
Règle qui contrôle les connexions liées à l'utilisation de Windows.

Personnalisée
Règle personnalisée.

< Précédent Suivant > Annuler

Cochez l'ensemble des règles et poursuivez.

Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

Quelles règles voulez-vous créer ?

Les règles suivantes définissent les besoins en connectivité réseau pour le groupe prédéfini sélectionné. Les règles qui sont cochées seront créées. Si une règle cochée existe déjà, son contenu sera remplacé.

Règles :

Nom	La règle existe...	Profil	Desc
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (LLMNR-...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Demand...	Non	Tout	Les n
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Demand...	Non	Tout	Les n
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Service ...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (service S...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (NB-Data...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (NB-Nom-...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (SMB-Ert...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (NB-Sessi...	Non	Tout	Règl

< Précédent

Suivant >

Annuler

Nous souhaitons autoriser ce flux alors sélectionnez "*Autoriser la connexion*".



Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :

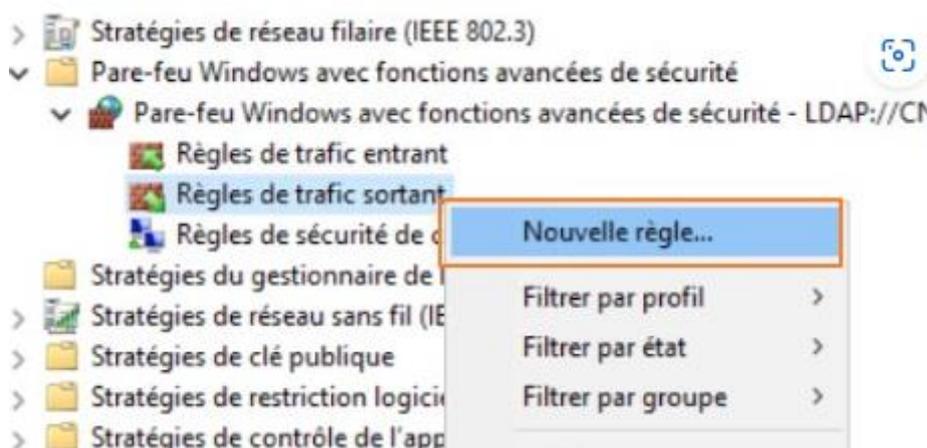
- Type de règle
- Règles prédéfinies
- Action

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

- Autoriser la connexion**
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.
- Autoriser la connexion si elle est sécurisée**
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.
- Bloquer la connexion**

< Précédent **Terminer** Annuler

Il va falloir recréer la même règle, mais pour le trafic sortant cette fois-ci, cliquez droit sur "*Règles de trafic sortant*" puis "*Nouvelle règle*".



Sélectionnez "*Prédéfinie*" puis "*Partage de fichiers et d'imprimantes*".

Assistant Nouvelle règle de trafic sortant

Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

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 :
Partage de fichiers et d'imprimantes
Règle qui contrôle les connexions liées à l'utilisation de Windows.

Personnalisée
Règle personnalisée.

< Précédent Suivant > Annuler

Cochez tout et continuez.



Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

Étapes :

- Type de règle
- Règles prédéfinies**
- Action

Quelles règles voulez-vous créer ?

Les règles suivantes définissent les besoins en connectivité réseau pour le groupe prédéfini sélectionné. Les règles qui sont cochées seront créées. Si une règle cochée existe déjà, son contenu sera remplacé.

Règles :

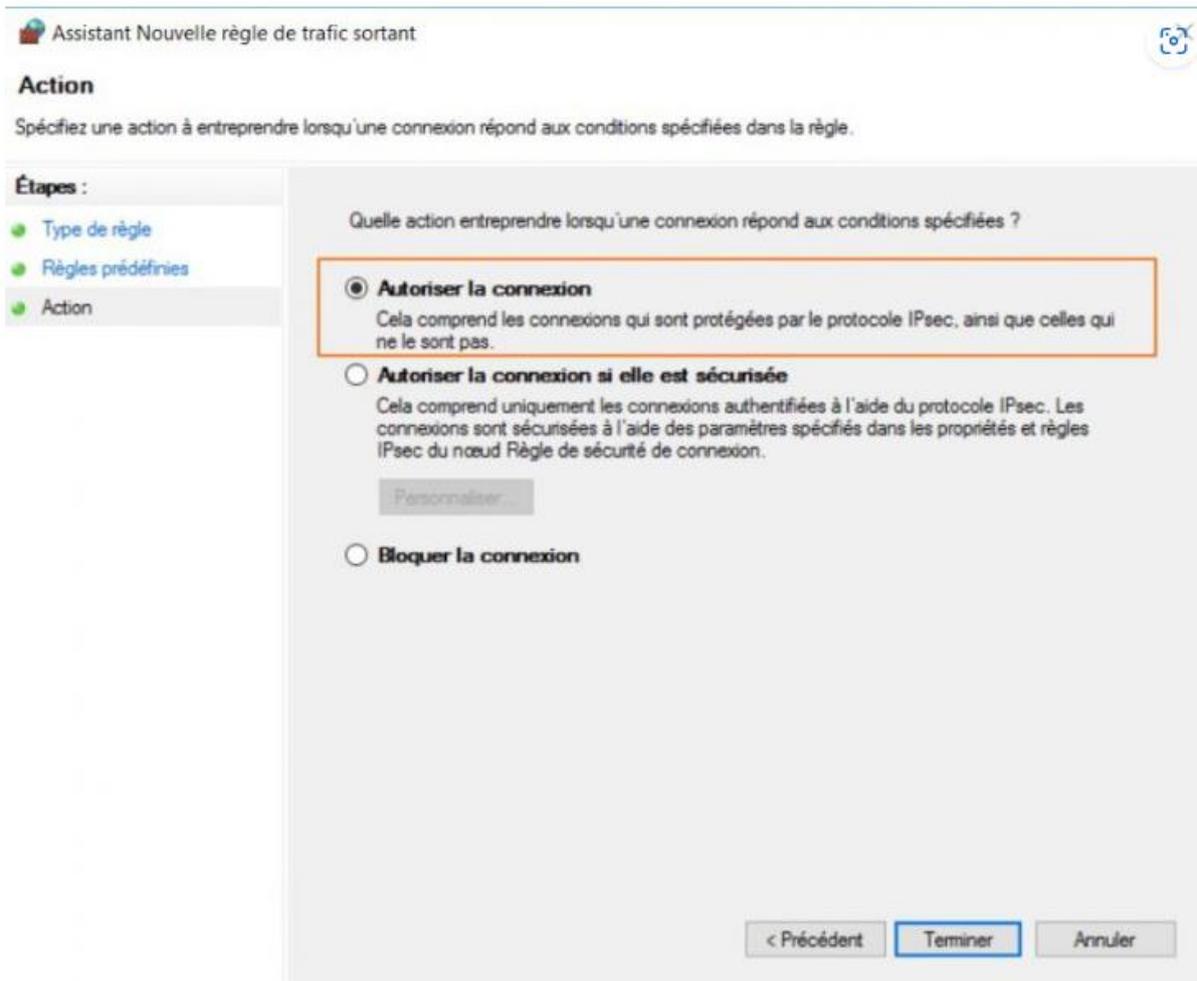
Nom	La règle existe...	Profil	Desc
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (LLMNR-...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Demand...	Non	Tout	Les n
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Demand...	Non	Tout	Les n
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (NB-Data...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (NB-Nom-...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (SMB-Sor...	Non	Tout	Règl
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (NB-Sessi...	Non	Tout	Règl

< Précédent

Suivant >

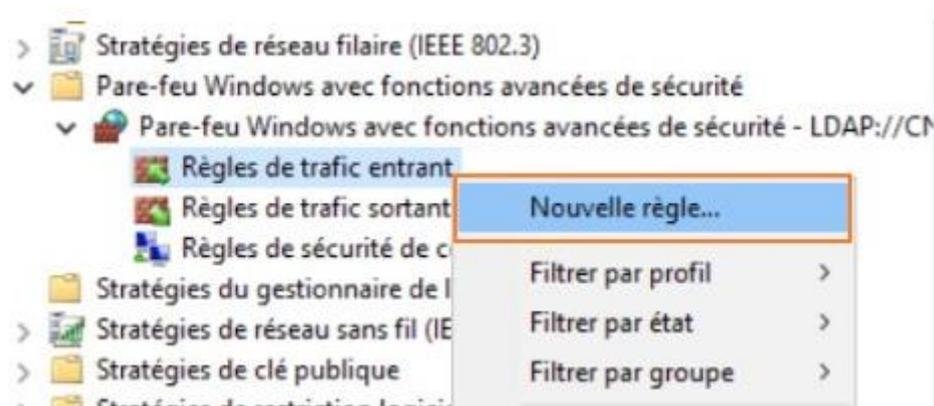
Annuler

Autorisez la connexion et finalisez la création de cette règle.

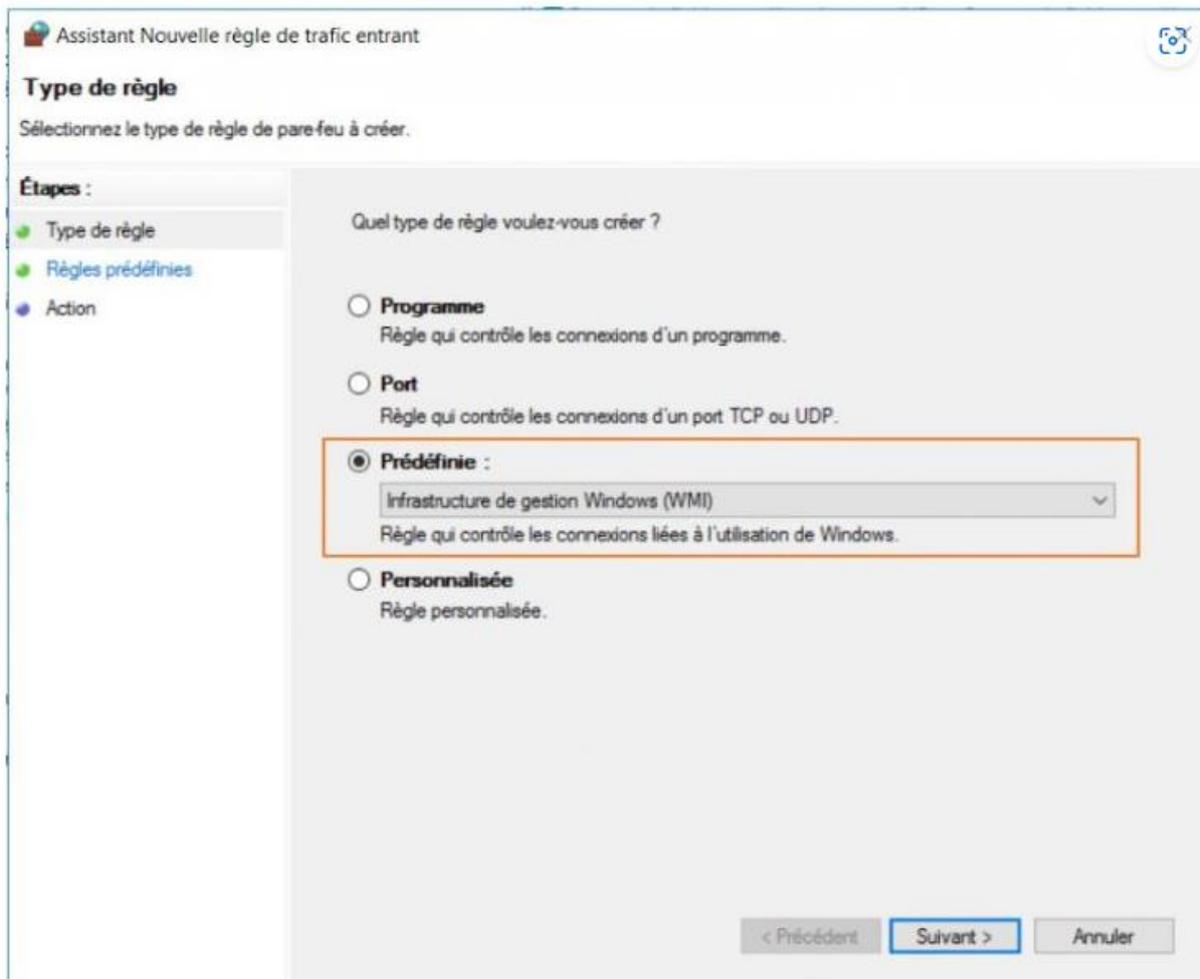


B. Règle "WMI"

Créez une nouvelle règle de trafic entrant :



Cette fois-ci, sélectionnez l'ensemble de règles prédéfinies **"Infrastructure de gestion Windows (WMI)"**.



Cochez les 3 règles et poursuivez.



Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

Quelles règles voulez-vous créer ?

Les règles suivantes définissent les besoins en connectivité réseau pour le groupe prédéfini sélectionné. Les règles qui sont cochées seront créées. Si une règle cochée existe déjà, son contenu sera remplacé.

Règles :

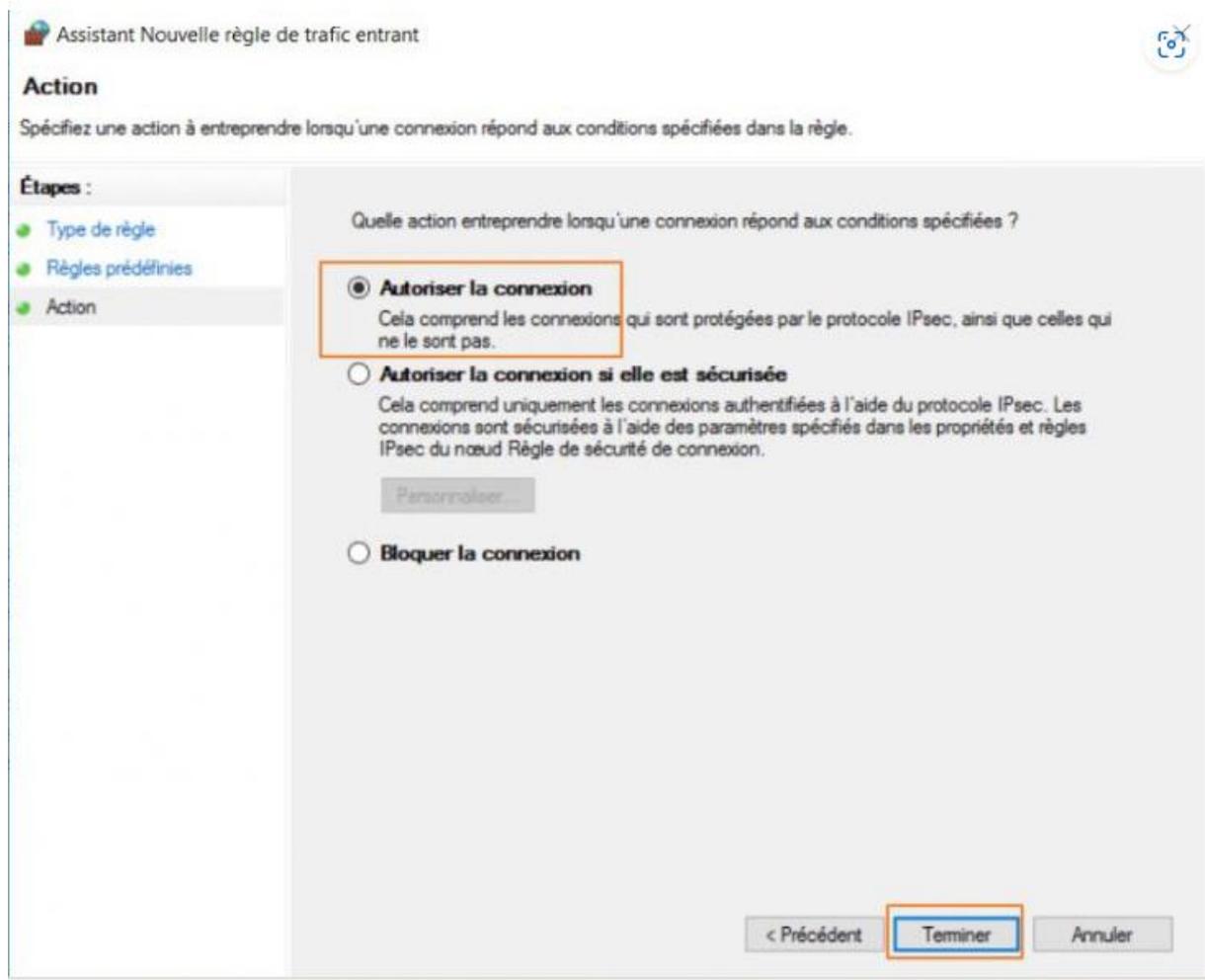
Nom	La règle existe...	Profil	Desc
<input checked="" type="checkbox"/> Windows Management Instrumentation (ASyn...	Non	Tout	Règl
<input checked="" type="checkbox"/> Windows Management Instrumentation (WMI-...	Non	Tout	Règl
<input checked="" type="checkbox"/> Windows Management Instrumentation (DCO...	Non	Tout	Règl

< Précédent

Suivant >

Annuler

Autorisez la connexion puis terminez la création de cet ensemble de règles.

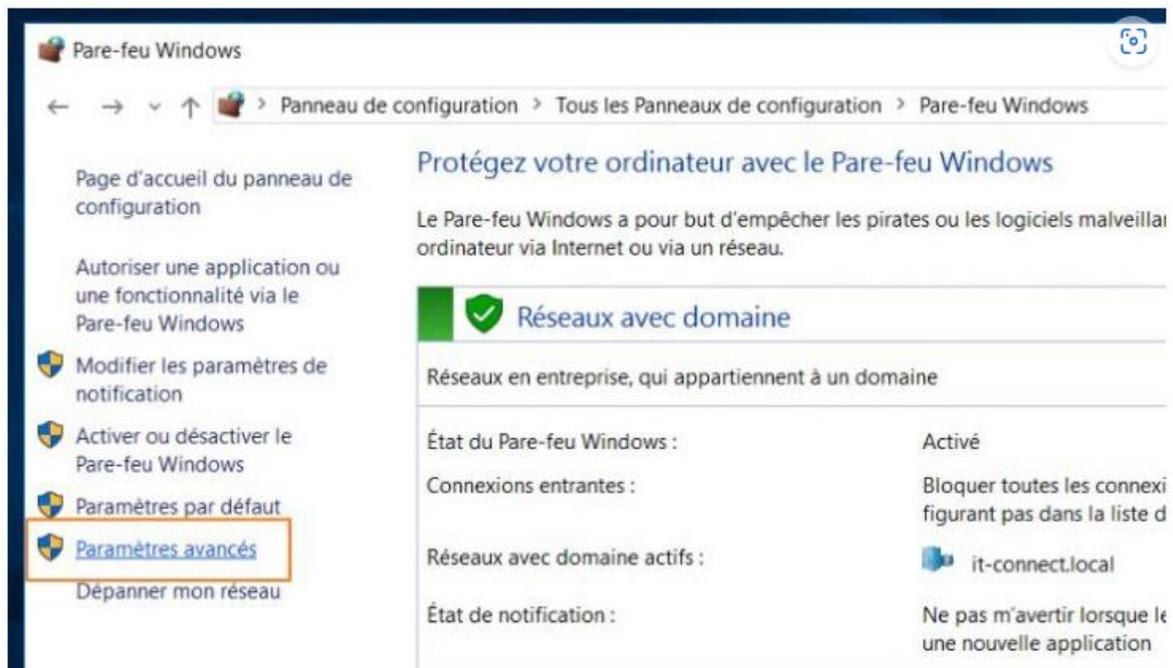


Il n'est pas nécessaire de refaire cette règle en trafic sortant, seulement en entrant c'est suffisant.

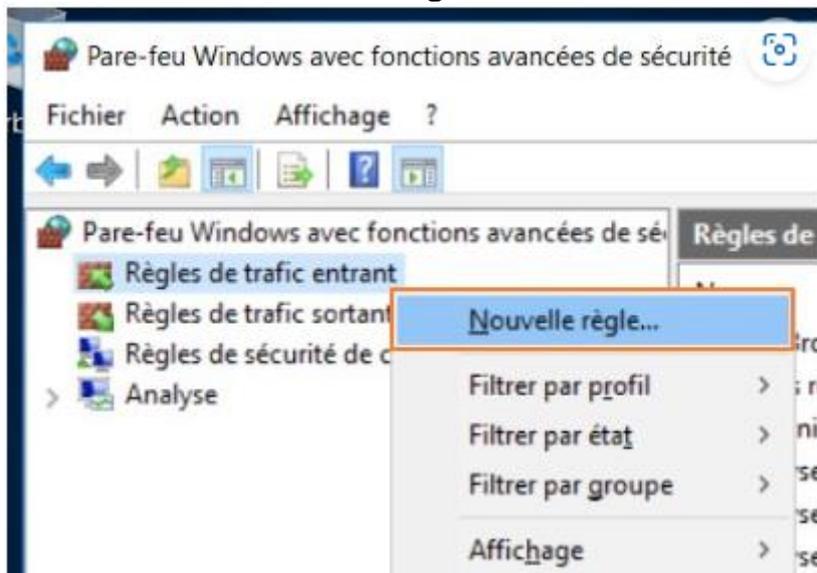
La GPO est terminée, il suffira de l'appliquer à l'ensemble des ordinateurs que vous gérez avec SCCM. Sur vos postes clients, il faudra réaliser l'habituel **"gpupdate /force"** pour forcer l'actualisation des GPO.

III. Ouverture des ports pour SQL Server

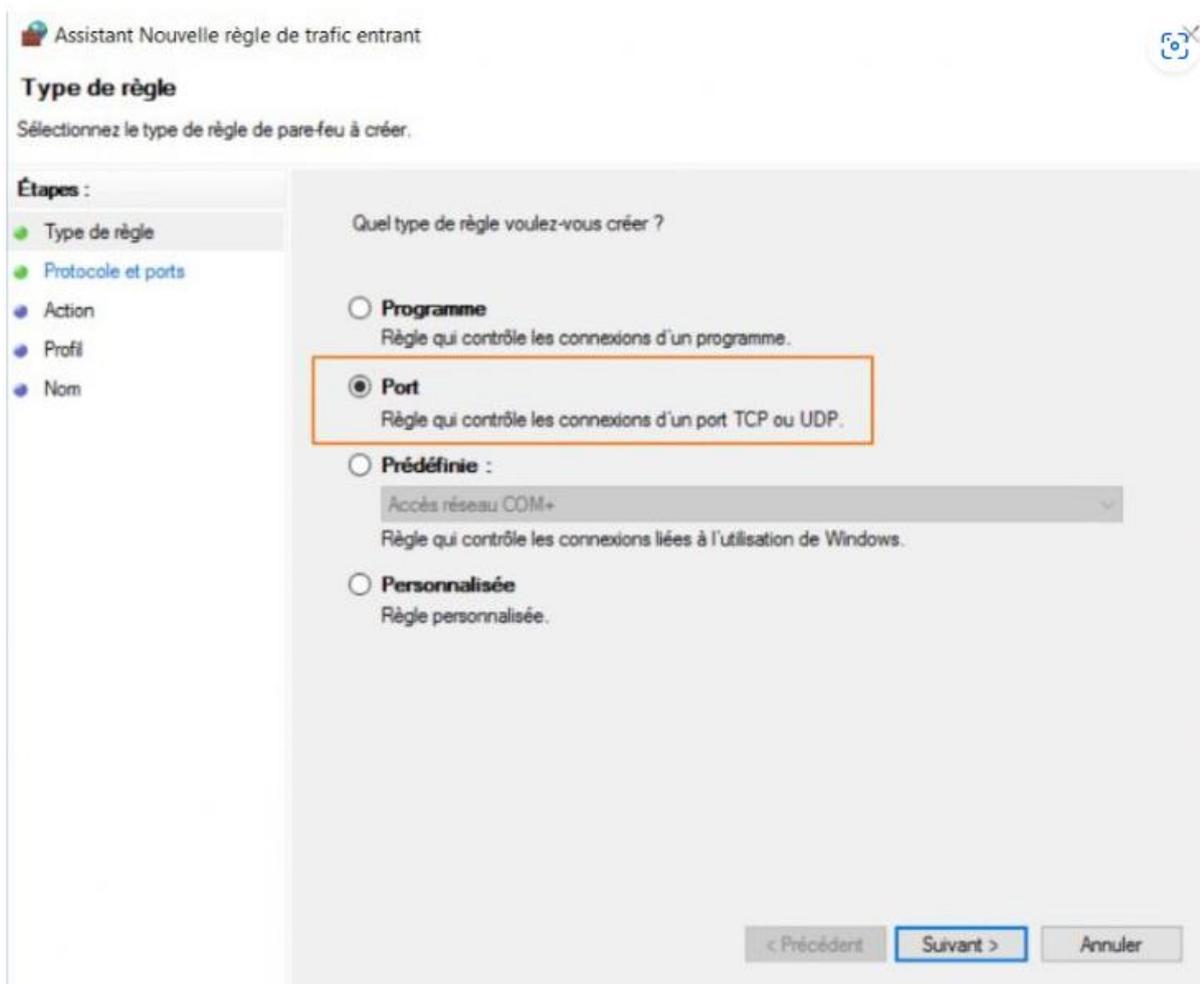
Étant donné que cette ouverture de ports concerne uniquement le serveur SQL, on va opérer directement depuis celui-ci. Je vous invite à aller dans le panneau de configuration, puis dans Pare-feu Windows. Sur la gauche, cliquez sur "*Paramètres avancés*".



Créez une nouvelle règle de trafic entrant :



Nous n'allons pas utiliser de règle prédéfinie cette fois-ci, car elle n'existe pas. Nous allons indiquer directement les ports que l'on souhaite ouvrir, sélectionnez "Port".



Cette règle s'applique au protocole "TCP" et la liste de ports est la suivante : 1433 et 4022.

Protocole et ports

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Cette règle s'applique-t-elle à TCP ou UDP ?

- TCP
 UDP

Cette règle s'applique-t-elle à tous les ports locaux ou à des ports locaux spécifiques ?

- Tous les ports locaux
 Ports locaux spécifiques :

1433, 4022

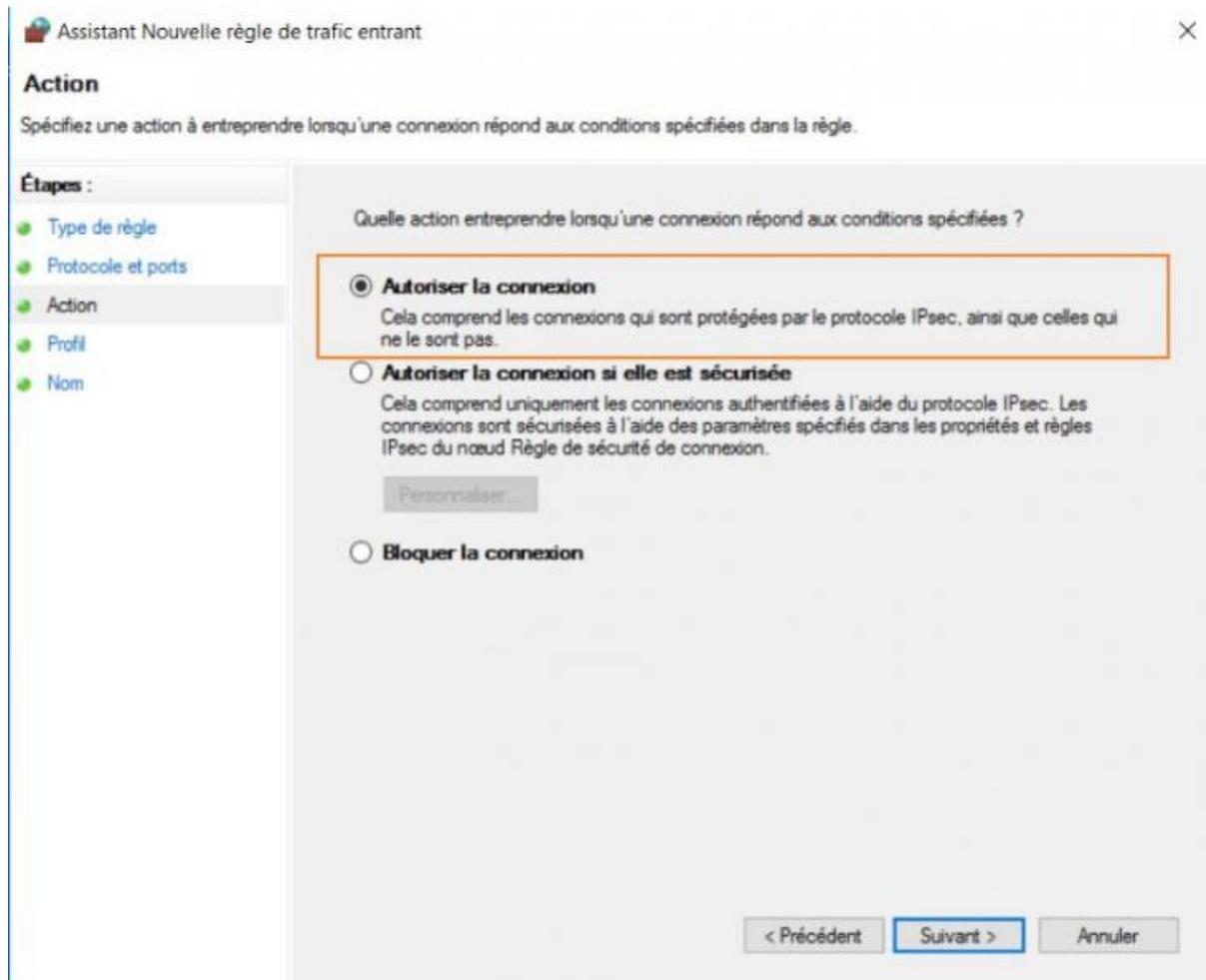
Exemple : 80, 443, 5000-5010

< Précédent

Suivant >

Annuler

Nous allons autoriser la connexion sur ces deux ports.



Pas besoin d'appliquer cette règle sur les profils privé et public, vous pouvez laisser seulement "Domaine". Comme ceci :



Profil

Spécifiez les profils auxquels s'applique cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Quand cette règle est-elle appliquée ?

- Domaine**
Lors de la connexion d'un ordinateur à son domaine d'entreprise.
- Privé**
Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.
- Public**
Lors de la connexion d'un ordinateur à un emplacement public.

< Précédent

Suivant >

Annuler

Nommez la règle, par exemple : **SCCM - SQL Ports 1433 et 4022**



Nom

Spécifier le nom et la description de cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Nom :

SCCM - SQL Ports 1433 et 4022

Description (facultatif) :

< Précédent

Terminer

Annuler

Tout est prêt sur le firewall