

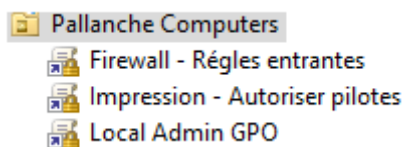
Règles entrantes PREDEFINIS crée à ce jour :

- **Règles nécessaires pour forcer la mise à jour de la stratégie de groupe :**

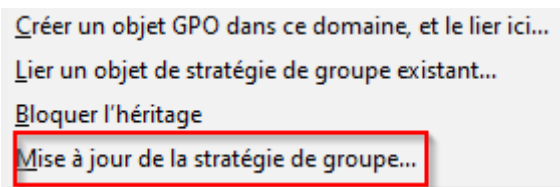
Infrastructure de gestion Windows

Gestion à distance des tâches planifiées

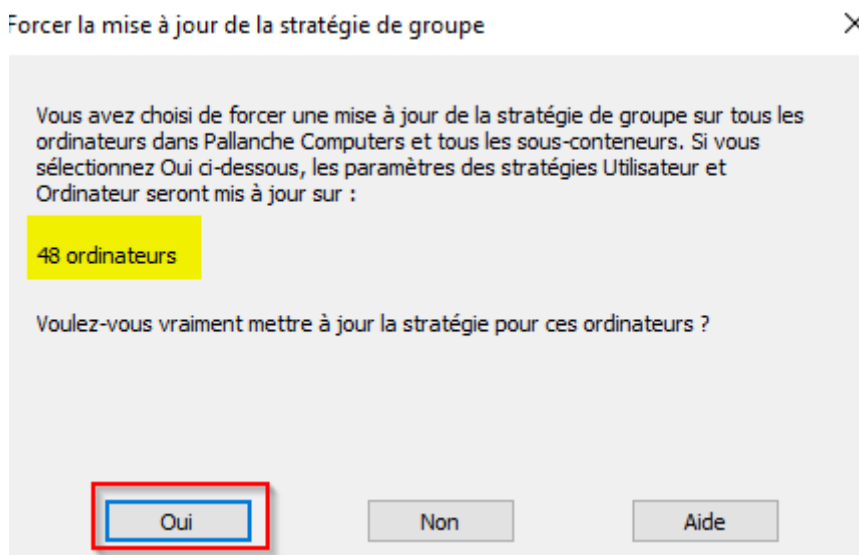
Après une création d'une GPO pour **ordinateurs**, un gpupdate ne suffit pas il faut forcer la mise à jour de la GPO (ou attendre 45 min).



Clique droite



Il nous indique le nombre d'ordinateur à qui la mise à jour va être forcer



Une mise à jour va se mettre en route et une erreur va s'afficher **si les 2 règles ne sont pas configurées**

La mise à jour de la stratégie de groupe sera forcée sur tous les ordinateurs dans IT - Computers et tous les sous-conteneurs au cours des dix prochaines minutes. Les paramètres de stratégie de l'utilisateur et de l'ordinateur seront actualisés.

Terminé (2 sur 2)

Nom de l'ordinateur	Code erreur	Description de l'erreur
Échec (2)		
W10-1903-CL1.IT-CONNECT.L...	8007071a	L'appel de procédure distante a été annulé.
W10-CL1.IT-CONNECT.LOCAL	8007071a	L'appel de procédure distante a été annulé.

Pour éviter l'erreur ont créer les 2 règles pour autoriser la mise à jour à distance

Réussite (1)

W10-CL1.IT-CONNECT.LOCAL

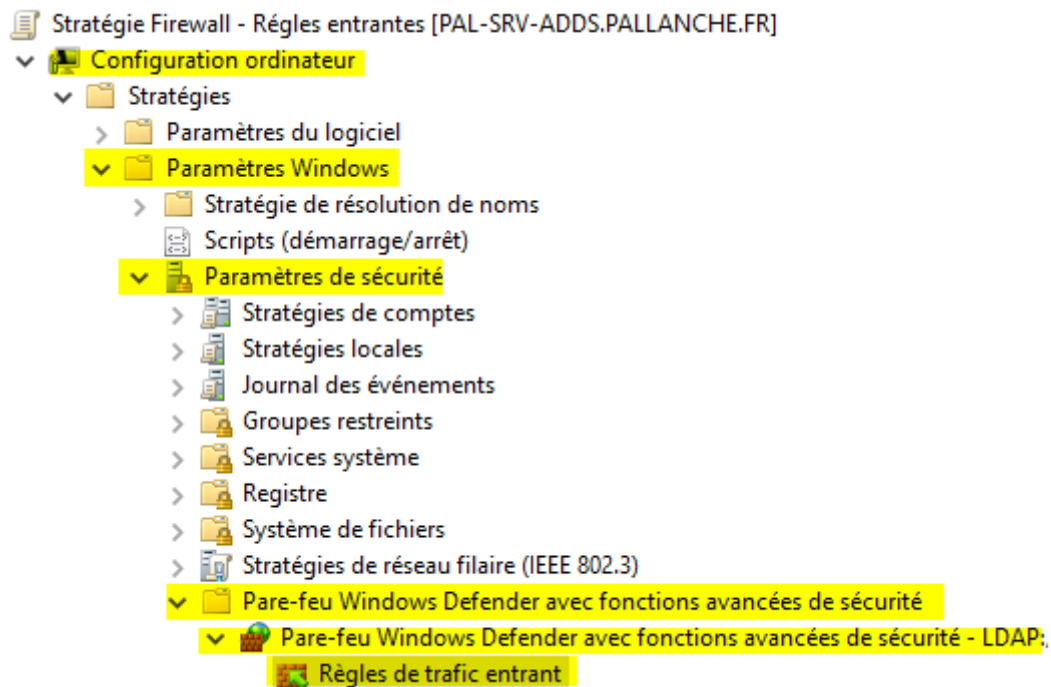
COTE UTILISATEURS ET ORDINATEURS

Aucune modification.

CONFIGURATION DE LA GPO

Modifier la GPO

Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Pare-feu Windows Defender avec ...\Pare-feu Windows Defender avec ...\Règles de trafic entrant



Clique Droit\Nouvelle règle

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 :**

Accès réseau COM+ ✓

Règle qui contrôle les connexions liées à l'utilisation de Windows.

Choisir UNE règle dans la liste

Accès réseau COM+

Active Directory Domain Services

Administration à distance COM+

Administration à distance du serveur de fichiers

Analyse de l'ordinateur virtuel

Arrêt à distance

BranchCache - Découverte d'homologue (utilise WSD)

BranchCache - Extraction du contenu (utilise HTTP)

BranchCache - Serveur de cache hébergé (utilise HTTPS)

Bureau à distance

Bureau à distance (WebSocket)

Centre de distribution de clés Kerberos

Coordinateur de transactions distribuées

Diagnostics de réseau de base

Équilibrage de charge logicielle

Fonctionnalité Diffuser sur un appareil

Gestion à distance de Windows

Gestion à distance de Windows (Compatibilité)

Gestion à distance des journaux des événements

Gestion à distance des tâches planifiées

Gestion à distance du Pare-feu Windows Defender

Gestion de carte à puce virtuelle TPM

Gestion des services à distance

Gestion des volumes à distance

Gestion du serveur DHCP

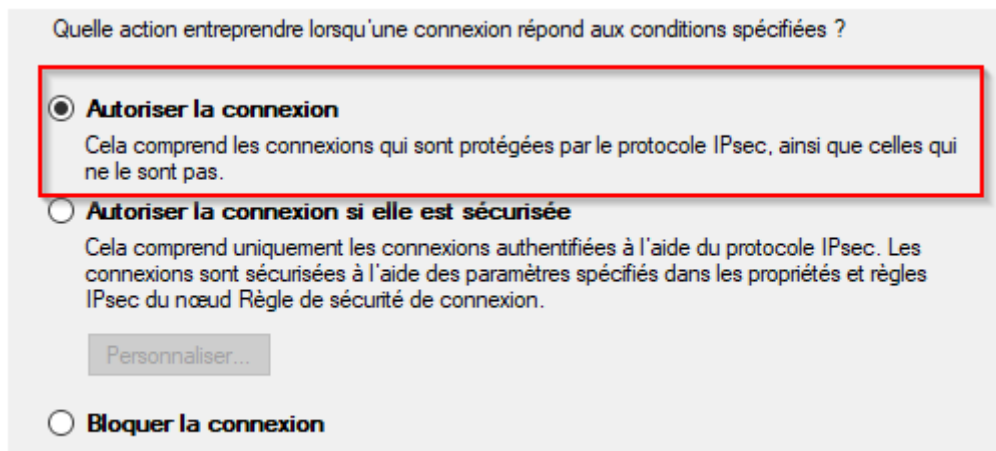
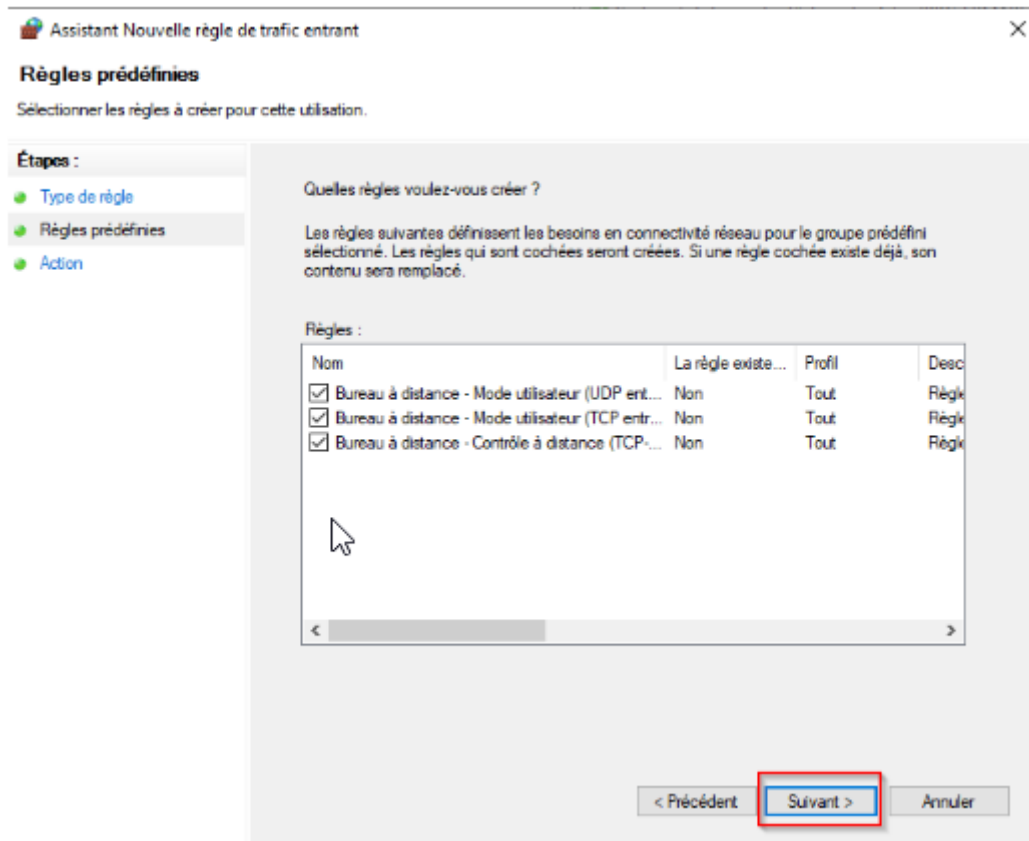
Gestion du système de fichiers distribués DFS

Infrastructure de gestion Windows (WMI)

Interruption SNMP

Journaux et alertes de performance

Lecteur Windows Media



Terminer

Refaire la configuration d'une nouvelle règle si on veut ajouter d'autre règle prédéfinis

Appliquer la GPO

CIBLAGE DE LA GPO

Aucun Ciblage

GPO liée à l'OU Pallanche Computers pour qu'elle s'applique à tous les PC du domaine

Appliquer la GPO

FONCTIONNEMENT DE LA GPO

La GPO s'applique à tous les ordinateurs du domaine. Elle permet de définir des règles entrantes sur le pare-feu Windows Defender de façon centraliser pour tous les pcs du domaine