L'Éditeur de stratégie de groupe

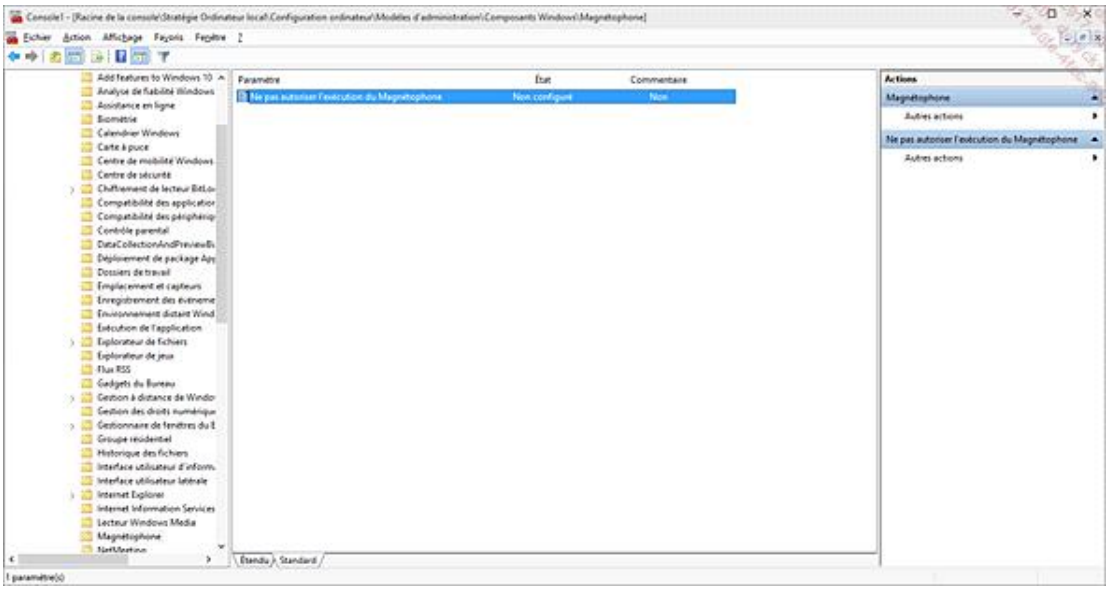
Ce composant vous permet notamment de manipuler un nombre considérable de paramètres du Registre. Voyons comment l'utiliser.

L'Éditeur est accessible depuis la console précédemment créée, ou en recherchant **Modifier la stratégie de groupe** dans la barre de recherche, ou en saisissant `gpedit.msc`.

1. Utiliser l'Éditeur de stratégie de groupe

Nous allons prendre un exemple simple :

- Ouvrez cette arborescence : **Stratégie Ordinateur local - Configuration ordinateur - Modèles d'administration - Composants Windows - Magnétophone**.
- Ouvrez cette stratégie : **Ne pas autoriser l'exécution du Magnétophone**.



- Cochez le bouton radio **Activé** puis cliquez sur **OK**.
- Essayez de lancer le Magnétophone en exécutant cette commande : `soundrecorder.exe`.

Un message vous avertira qu'il est impossible d'ouvrir ce programme car il est protégé par une stratégie de restriction logicielle.

Il est possible de désactiver cette stratégie ou de la supprimer en cochant le bouton radio **Non configuré**.

- Refaites maintenant la même manipulation dans l'arborescence **Ordinateur local - Non-administrateurs**.

Vous pourrez ouvrir le Magnétophone mais, si vous essayez cette même commande à partir d'un compte d'utilisateur ne disposant pas de privilèges d'administrateur, vous obtiendrez le même message d'erreur que précédemment.

- Désactivez de nouveau cette stratégie.
- Ouvrez l'arborescence **Stratégie ordinateur local - Configuration utilisateur - Modèles d'administration - Composants Windows - Magnétophone**.
- Activez la même stratégie puis essayez de lancer le Magnétophone.

Vous obtiendrez le même message d'erreur. Il en sera de même à partir d'un compte d'utilisateur.

Nous pouvons donc en conclure que vous ne pourrez pas appliquer des stratégies "machine" en distinguant les utilisateurs qui ouvriront une session localement.

Il est possible de filtrer les stratégies de cette façon :

- Ouvrez une des branches présentes (uniquement dans **Modèles d'administration**).
- Effectuez un clic droit dessus puis cliquez sur les sous-menus **Affichage** et **Options des filtres...**.

Vous pouvez :

- **Filtrer sur le type de paramètre de stratégie à afficher** : permet de ne lister que les stratégies qui sont activées.
- **Filtrer par mots clés** : permet de ne lister que les stratégies qui contiennent un ou plusieurs mots-clés dans le titre, le texte d'explication ou le commentaire associé.
- **Filtrer par paramètres de conditions** : permet de ne lister que les stratégies qui ne s'appliquent qu'avec tel ou tel système d'exploitation ou avec telle ou telle application.

A priori, cette option ne concerne que les stratégies que vous pourrez configurer en créant des fichiers ADMX personnalisés.

Les fichiers ADMX sont la nouvelle version des modèles d'administration (*.adm) en vigueur sous Windows XP. Ce sont des fichiers de modèles au format XML qui contiennent les informations et les paramètres de Registre propres à chacune des stratégies listées dans l'Éditeur d'objets de stratégie de groupe.

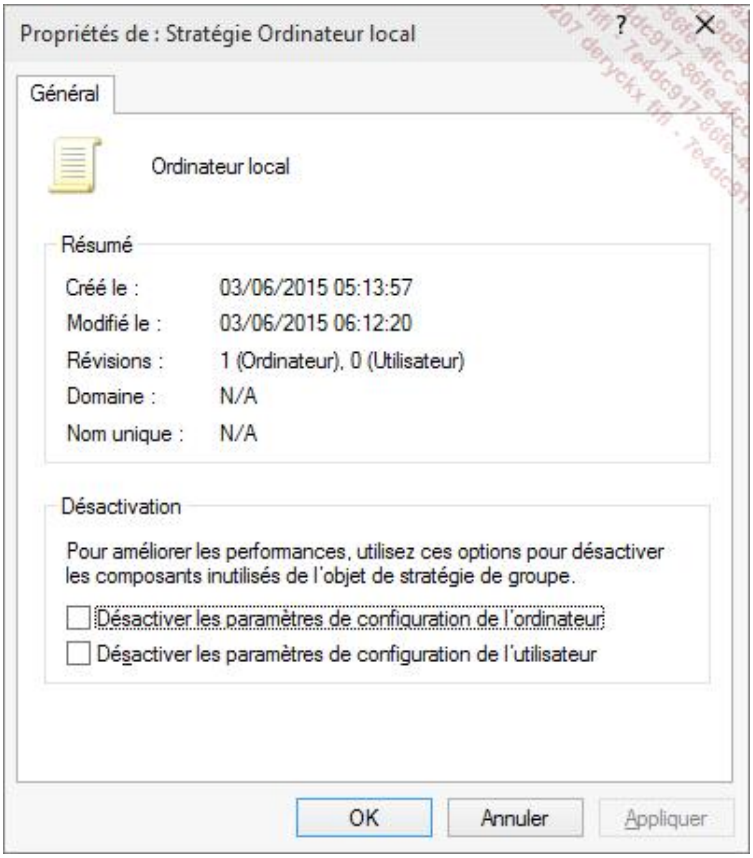
Notez que les branches du Registre qui sont modifiées sont principalement au nombre de quatre :

- **HKEY_LOCAL_MACHINE - SOFTWARE - Policies**
- **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows - CurrentVersion - Policies**
- **HKEY_CURRENT_USER - Software - Policies**
- **HKEY_CURRENT_USER - Software - Microsoft - Windows - CurrentVersion - Policies**

Afin de désactiver l'ensemble des stratégies que vous aurez configurées, effectuez un clic droit sur le nœud **Stratégie Ordinateur local** puis cliquez sur le sous-menu **Propriétés**.

Cochez l'une ou l'autre ou même les deux cases suivantes :

- **Désactiver les paramètres de configuration de l'ordinateur**
- **Désactiver les paramètres de configuration de l'utilisateur**



2. Appliquer une stratégie pour tous les autres utilisateurs de votre machine

- Ouvrez une session sur votre compte.
- Activez les stratégies dans l'arborescence **Configuration utilisateur**.
- Fermez puis ouvrez de nouveau votre session interactive.
- Vérifiez que les stratégies que vous avez configurées s'appliquent bien à vous.

Vous pouvez également tester leur efficacité à partir des autres comptes d'utilisateurs.

- Copiez le fichier \Windows\System32\GroupPolicy\User\Registry.pol dans votre dossier d'utilisateur.
- Ouvrez de nouveau l'Éditeur d'objets de stratégie de groupe puis désactivez toutes les stratégies que vous avez au préalable activées.

Il peut être plus simple d'activer le filtre permettant de n'afficher que les stratégies configurées.

- Fermez l'Éditeur d'objets de stratégie de groupe.
- Copiez le fichier que vous avez sauvegardé dans son répertoire d'origine en confirmant le remplacement du fichier existant.
- Fermez puis ouvrez de nouveau votre session d'utilisateur.

Vous pourrez constater que les stratégies activées ne s'appliquent plus à votre compte.

- Ouvrez une session sur les autres comptes d'utilisateurs afin de vérifier que les stratégies continuent bien à s'appliquer aux autres comptes.

3. Restaurer les stratégies locales d'origine

- Supprimez le même fichier *Registry.pol*.
- Ouvrez l'Éditeur d'objets de stratégies de groupe et paramétrez toutes les stratégies sur le mode **Non configuré**.
- Fermez puis ouvrez de nouveau les sessions des utilisateurs.

Les stratégies auront toutes été désactivées.

4. Afficher les stratégies résultantes

Cet outil vous permet d'afficher rapidement les stratégies qui peuvent résulter d'une GPO (*Group Policy Object*) propre à un domaine, un réseau local, un groupe d'utilisateurs, un utilisateur, et vous aide à détecter d'éventuels problèmes ou planifier de nouveaux paramètres.

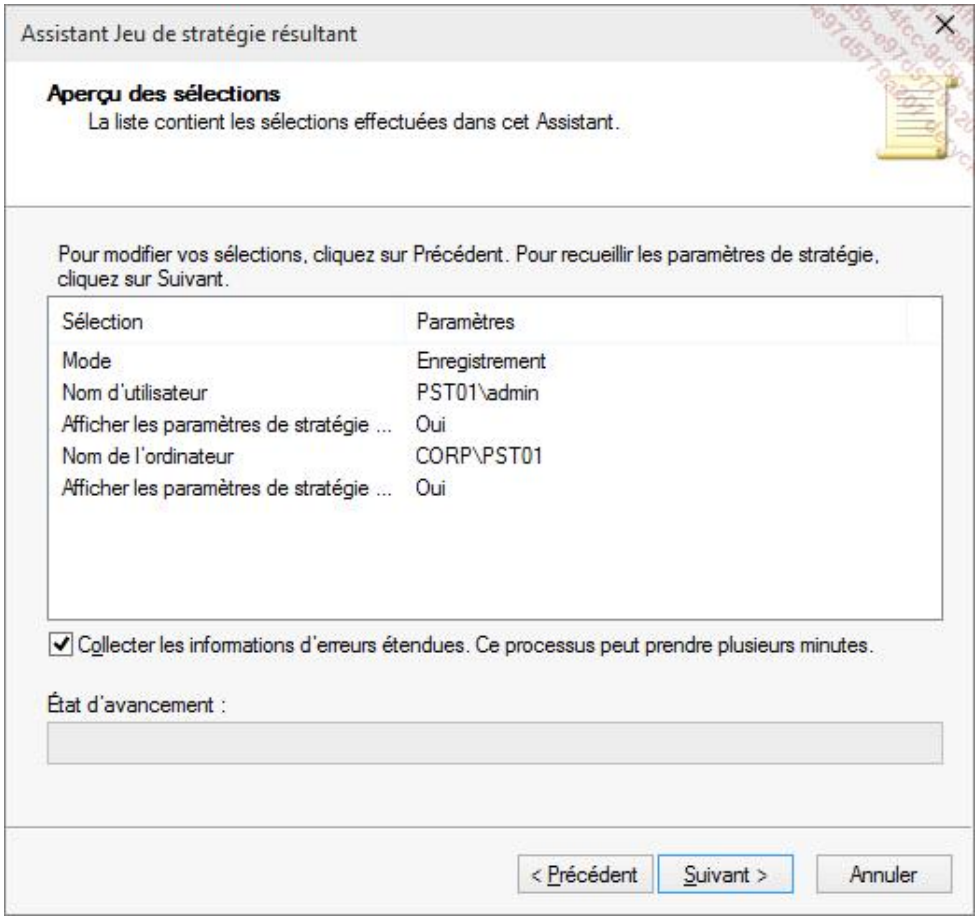
- Ajoutez le composant logiciel suivant : **Jeu de stratégie résultant**.
- Effectuez un clic droit sur ce composant puis cliquez sur le sous-menu **Générer les données RSoP**.
- Cliquez deux fois sur **Suivant**.

Vous avez le choix entre :

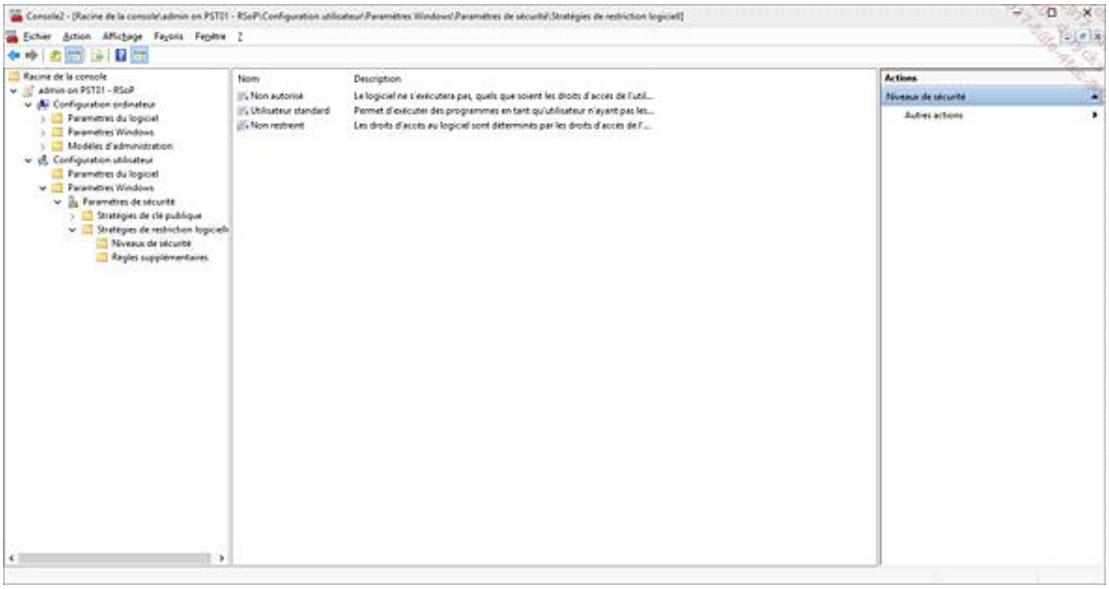
- **Afficher les stratégies de cet ordinateur ou d'un autre ordinateur**
- **Afficher uniquement les paramètres de la stratégie de l'utilisateur.**

Dans ce dernier cas, laissez coché le bouton radio **Utilisateur actuel** ou sélectionnez un des utilisateurs listés en dessous.

- Validez pour le reste.



Les stratégies qui s'appliquent à l'utilisateur que vous aurez sélectionné seront affichées.



Le pare-feu de connexion Internet

Un pare-feu de connexion internet (ou firewall) est un dispositif logiciel ou matériel qui vérifie les données entrantes ou sortantes qui vont ou viennent des réseaux externes comme Internet. Un pare-feu vous permet donc de vous prémunir des attaques de hackers ou de programmes malveillants qui tentent de prendre le contrôle d'une manière ou d'une autre de votre système. Voyons comment fonctionne le pare-feu de connexion internet intégré à Windows. Mais auparavant, nous devons nous intéresser aux notions de port et de protocole.

1. Ports et protocoles réseau

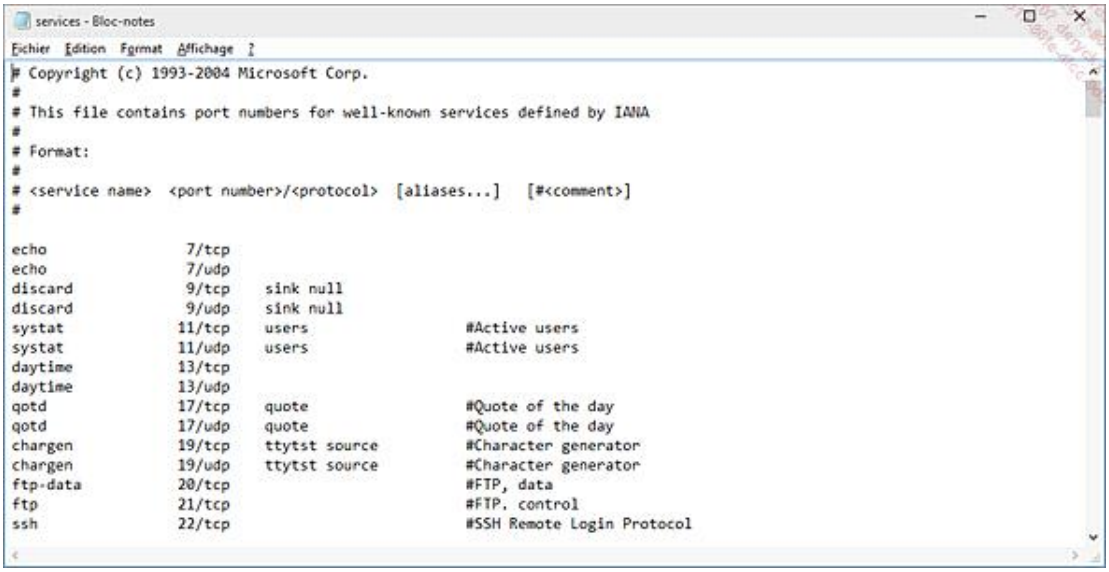
Un protocole réseau est un ensemble de règles pour un type de communication défini. Les protocoles les plus connus sont :

- FTP (*File Transfer Protocol*) utilisé pour les échanges de fichiers sur Internet.
- HTTP (*Hypertext Transfer Protocol*) : servant pour les navigateurs web à utiliser Internet.
- SMTP (*Simple Mail Transfer Protocol*) : servant à transférer le courrier électronique vers les serveurs de messagerie.
- UDP (*User Datagram Protocol*) : utilisé par Internet et faisant partie de la couche transport de la pile de protocole TCP/IP.
- TCP (*Transmission Control Protocol*) est un protocole de contrôle de transmissions des données à l'instar d'UDP.

Quand une application initie une connexion entrante ou sortante, elle utilise donc un protocole auquel sont associés un ou plusieurs numéros de ports. Nous allons donc expliquer cette seconde notion… En programmation, un port est le nom attribué à une connexion de type logique qui est utilisée par un protocole. On peut donc le définir comme une porte qui est laissée ouverte ou fermée dans votre système d'exploitation. Vous pouvez imaginer un immeuble à plusieurs étages, chaque étage disposant d'une porte d'entrée : un seul édifice, mais plusieurs portes…

En d'autres termes, une application comme votre navigateur internet va utiliser un ou plusieurs protocoles et un ou plusieurs ports pour communiquer avec l'extérieur. En sens inverse, une application s'exécutant à partir d'une machine distante peut avoir besoin qu'un ou plusieurs ports soient ouverts sur votre ordinateur afin d'accomplir certaines tâches comme, par exemple, l'installation d'une mise à jour.

Afin d'avoir une liste des ports qui sont définis sur votre machine, il vous suffit d'exécuter cette commande : `notepad %SystemRoot%\system32\drivers\etc\services`.



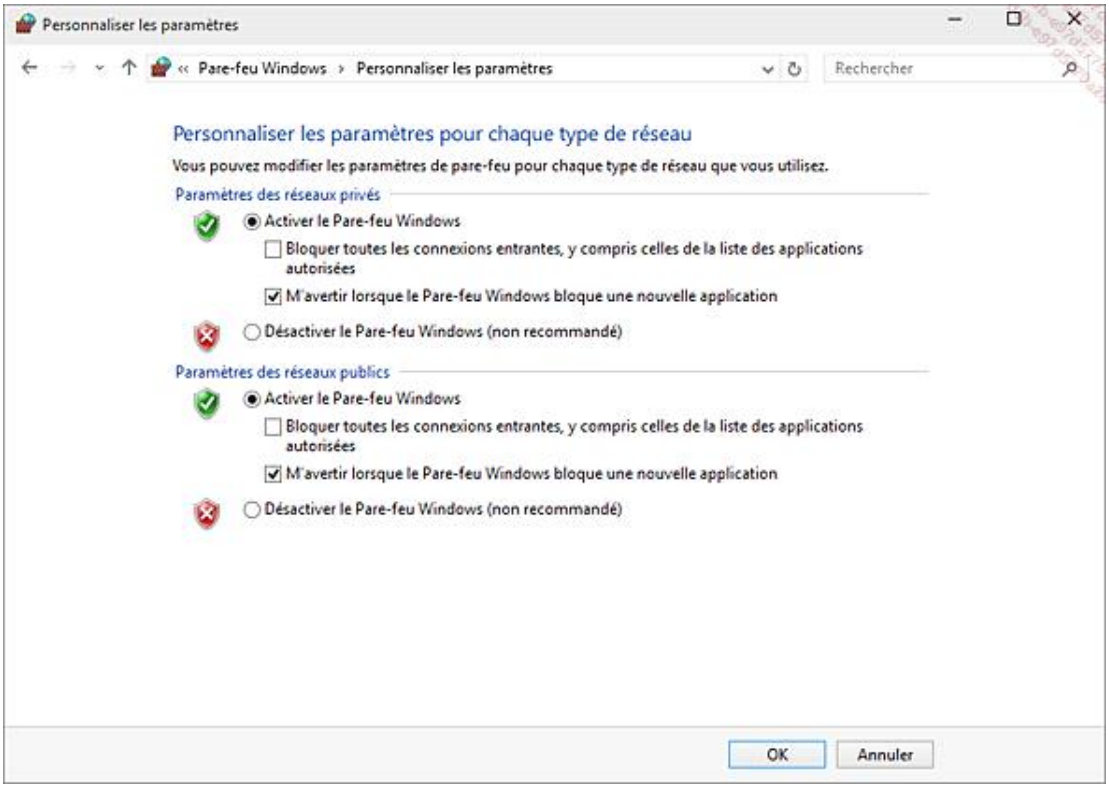
En conclusion, un pare-feu de connexion est un programme chargé de limiter les entrées qui sont ouvertes dans votre système afin d'offrir la meilleure sécurité possible. Par défaut, un pare-feu empêche toute connexion entrante et sortante, à moins que certaines exceptions n'aient été définies. Cela consiste simplement à édicter une règle qui, par exemple, va attribuer à telle application la possibilité d'ouvrir tel port en utilisant tel protocole. Prenons un exemple : vous utilisez le logiciel de Peer-To-Peer eMule et constatez que les taux de transfert sont extrêmement lents. De plus, l'icône du programme vous indique qu'il vous a été attribué un ID faible. Cela provient simplement du fait qu'eMule utilise deux ports aléatoires par défaut (anciennement les ports 4662 et 4672) et que vous devez par conséquent les ouvrir dans votre pare-feu de connexion Internet en créant une règle pour cette application.

2. Paramétrer le Pare-feu Windows

Avec Windows 10, le pare-feu fait partie intégrante du système et a été intégré dans **Sécurité Windows**, section des **Paramètres** qui regroupe tous les paramètres gérant la sécurité de votre système.

Sous Windows, le pare-feu est lié au type d'emplacement réseau. Le pare-feu est, par défaut, activé pour les réseaux de type domestique ou d'entreprise et pour les réseaux de type public.

À partir du **Panneau de configuration**, dans la section **Système et sécurité** - **Pare-feu Windows**, cliquez sur l'option **Activer ou désactiver le Pare-feu Windows**.

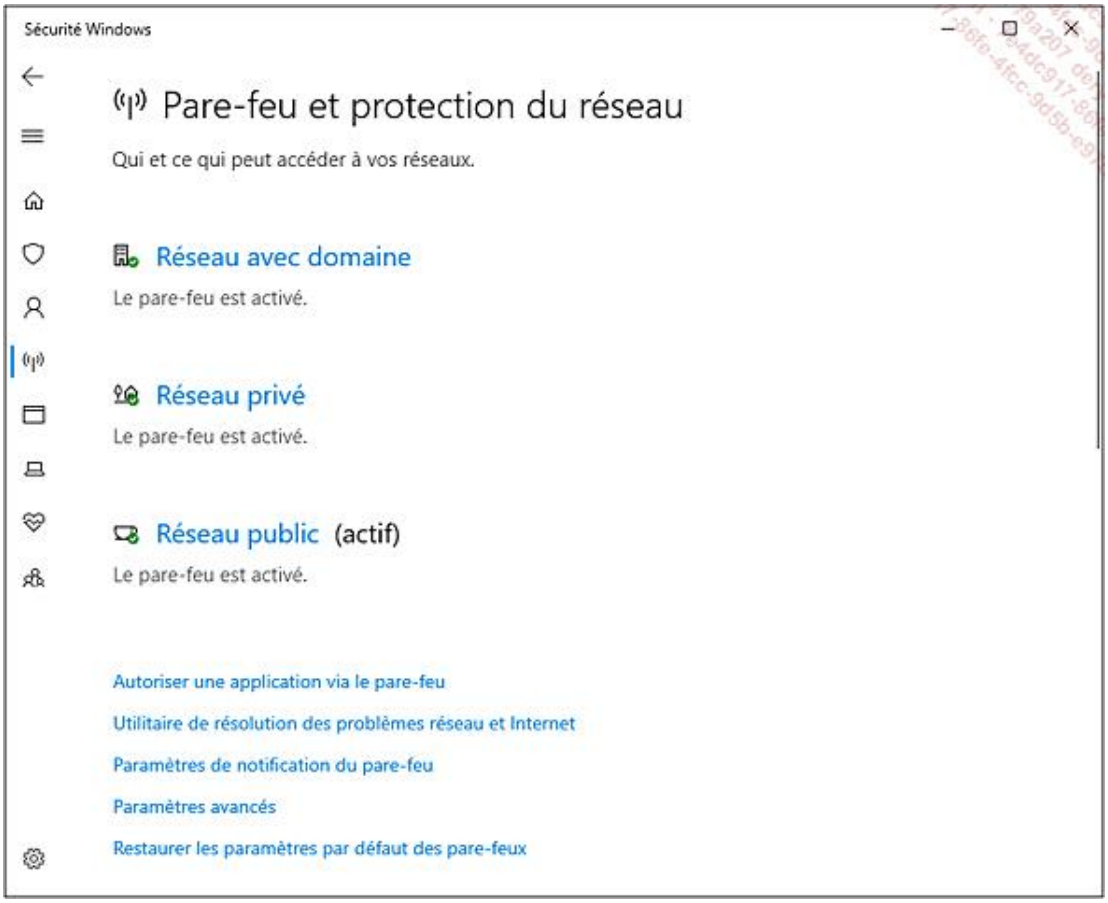


Pour chaque type d'emplacement réseau, vous avez le choix entre trois options :

- **Activer** : ce paramètre empêche toutes les sources extérieures de se connecter à votre machine, sauf les applications que vous aurez spécifiées dans l'onglet **Exceptions**.
- **Bloquer toutes les connexions entrantes** : toutes les exceptions que vous aurez définies seront ignorées et aucun message ne vous avertira quand le Pare-feu Windows bloquera des programmes.
- **Désactiver** : cochez ce bouton radio si vous avez installé un pare-feu provenant d'un autre éditeur ou que vous disposez d'un modem/routeur.

  Vous pouvez retrouver les mêmes réglages depuis la fenêtre des **Paramètres - Mise à jour et sécurité - Sécurité**

Windows, en ouvrant **Pare-feu et protection du réseau**.



3. Gérer les exceptions

Par défaut, seules les connexions entrantes sont vérifiées. Si par contre un de vos programmes tente de communiquer avec l'extérieur, il peut le faire sans aucune vérification des données transmises. Le raisonnement sous-jacent consiste à dire que si votre système est correctement protégé au niveau des connexions entrantes, il n'est nul besoin de vérifier les connexions sortantes !

Dès que vous installez un programme qui nécessite une connexion entrante, il sera automatiquement ajouté à votre liste d'exceptions. Afin d'autoriser ou de supprimer une des exceptions qui sont déjà paramétrées, il suffit de cocher ou de décocher la case correspondante.

Sous Windows, la notion d'exception n'est pas explicite. La fonction est accessible :

- Depuis la section **Pare-feu Windows** du **Panneau de configuration**, en cliquant sur le lien **Autoriser une application ou une fonctionnalité via le Pare-feu Windows**.
- Depuis la section **Pare-feu et protection du réseau** de **Sécurité Windows**, en cliquant sur **Autoriser une application via le pare-feu**.

4. Utilisation avancée du pare-feu de connexion internet

Afin d'accéder aux paramètres avancés de cet outil, suivez cette procédure :

- Cliquez sur **Démarrer** - **Panneau de configuration**, puis ouvrez le module **Outils d'administration**.

- Ouvrez la branche **Pare-feu Windows avec fonctions avancées de sécurité**.

Vous pouvez aussi directement exécuter cette commande : `wf.msc`.

- Il existe une troisième manière d'y accéder : depuis les **Paramètres**, ouvrez **Mise à jour et sécurité - Sécurité Windows - Ouvrir Sécurité Windows**, puis dans la nouvelle fenêtre qui apparaît, ouvrez **Pare-feu et protection du réseau** et cliquez sur **Paramètres avancés**.

Ce composant logiciel enfichable vous permet de filtrer les connexions entrantes et sortantes ainsi que les paramètres IPsec que vous aurez définis. Rappelons que IPsec (*Internet Protocol Security*) est un ensemble de protocoles permettant de sécuriser des échanges de données sur un réseau. Trois profils sont définis :

- Un profil de domaine si votre ordinateur est connecté à un serveur de domaine Windows.
- Un profil privé si vous êtes connecté à un réseau privé.
- Un profil public si, par exemple, vous êtes connecté sur un réseau sans fil d'un aéroport ou d'un hôtel.

Les règles possibles sont au nombre de trois :

- **Règles de trafic entrant** : ces règles régissent le trafic entrant vers votre machine.
- **Règles de trafic sortant** : ces règles définissent comment est configuré le trafic sortant à partir de votre machine.
- **Règles de sécurité de connexion** : elles servent à utiliser des règles d'authentification quand deux ordinateurs communiquent entre eux. Les technologies IPsec permettent de paramétrer les échanges de clé, les méthodes d'authentification, la vérification et l'encryptage des données.

5. Fonctionnement des règles de sécurité avancées

Les règles (clic droit sur l'une d'elle, sous-menu **Propriétés**, onglet **Général**) vous permettent de :

- **Autoriser la connexion**.
- **Autoriser la connexion seulement si elle est sécurisée** (à travers l'utilisation d'un protocole Internet sécurisé IPsec).
- **Bloquer une connexion**.

Il est possible de les configurer pour qu'elles ne concernent qu'un utilisateur, une machine, un programme, un service, un port ou un protocole en particulier. Vous pouvez également définir à quelle interface réseau elle s'applique : réseau local (LAN), connexion sans fil, accès à distance, etc. Elles seront appliquées dans cet ordre :

- Règles de sécurité de connexion.
- Règles dites "de blocage".
- Règles "Autoriser".

Un grand nombre de règles sont déjà prédéfinies :

- L'absence d'icône bouton signale que la règle n'est pas active.
- Une petite icône de coche verte indique que la règle est active et la connexion autorisée.
- Une petite icône rouge barrée indique que la règle est active et la connexion bloquée.

Les colonnes placées dans le volet central affichent les éléments suivants :

- **Nom** : indique le nom de la règle.
- **Groupe** : indique le nom du groupe dont fait partie la règle.
- **Profil** : indique le domaine privé, public ou tout.
- **Activé** : indique si la règle est active ou non.
- **Action** : indique si la règle est une règle de blocage ou non.
- **Programme** : indique l'emplacement et le nom du fichier exécutable qui est visé par la règle.
- **Adresse locale** : indique l'adresse IP sur laquelle s'applique la règle.
- **Adresse distante**: indique l'adresse IP ou la plage d'adresses IP des machines distantes concernées par la règle.
- **Protocole** : indique le protocole défini par la règle (TCP ou UDP).
- **Port local** : indique le numéro de port utilisé localement par l'application cible.
- **Port distant** : indique les ports utilisés par les machines distantes quand elles sollicitent l'application qui est définie.
- **Utilisateurs autorisés** : indique quels sont les utilisateurs concernés par la règle sélectionnée.
- **Ordinateurs autorisés** : indique quels sont les ordinateurs concernés par la règle sélectionnée.
- **Entités de sécurité locales autorisées** : indique si la règle s'applique à tout ou partie des entités de sécurité locales, comme par exemple les utilisateurs locaux.
- **Propriétaire des utilisateurs locaux** : indique le propriétaire de la règle de sécurité. S'applique en particulier aux applications du Windows Store.
- **Package d'application** : indique l'application du Windows Store pour laquelle la règle s'applique.

→ Double cliquez sur chacun des en-têtes de colonne si vous souhaitez filtrer les différentes listes en fonction des valeurs présentes.

Nous allons prendre un exemple simple en examinant comment autoriser les requêtes PING vers votre ordinateur. Cette commande permet d'envoyer une requête d'écho vers une autre machine. Si cette dernière ne répond pas, il est possible que les deux ordinateurs ne puissent pas communiquer entre eux.

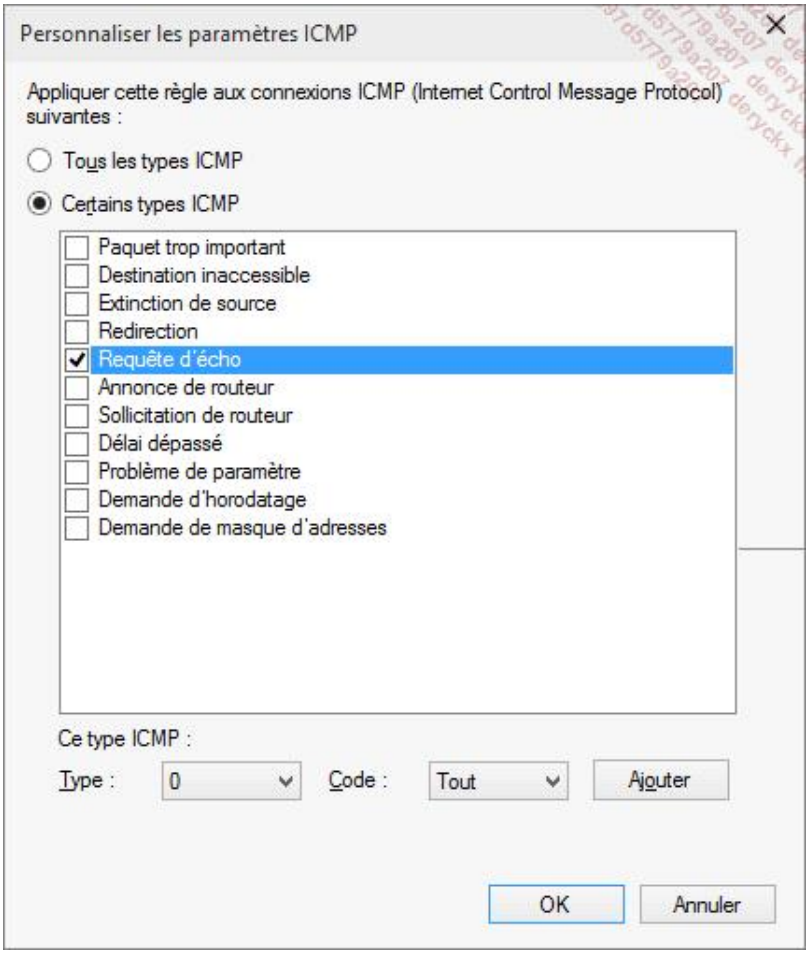
→ Effectuez un clic droit sur la branche **Règles de trafic entrant**, puis cliquez sur le sous-menu **Nouvelle règle...**

→ Sélectionnez le bouton radio **Personnalisée**, puis cliquez sur **Suivant**.

→ Sélectionnez le bouton radio **Tous les programmes**, puis cliquez sur **Suivant**.

→ Dans la liste déroulante **Type de protocole**, sélectionnez l'option **ICMPv4**, puis cliquez sur le bouton **Perso...**.

→ Cochez le bouton radio **Certains types ICMP**, puis cochez la case **Requête d'écho**.



- Cliquez sur les boutons **OK** et **Suivant**.
- Définissez éventuellement quelles sont les adresses IP locales et les adresses IP des machines distantes.
- Cliquez deux fois sur **Suivant**.
- Définissez dans quel environnement cette règle sera appliquée, puis cliquez sur **Suivant**.
- Saisissez un nom et une description pour cette règle, puis cliquez sur **Terminer**.

6. Gestion avancée du pare-feu en ligne de commande

L'utilisation de commandes avancées pour la gestion du pare-feu permet d'automatiser les tâches de configuration ou d'intervenir à distance, mais aussi de rapidement lister les informations utiles pour relever la configuration du pare-feu.

Depuis une invite de commandes en mode administrateur, tapez la commande suivante pour déterminer les profils actifs :

```
netsh advfirewall show allprofiles
```

Pour interroger l'ensemble des règles configurées pour le profil public, tapez la commande suivante :

```
netsh advfirewall firewall show rule name=all profile=public
```