Utilisation du pare-feu Windows

M. Tellene

Table des matières

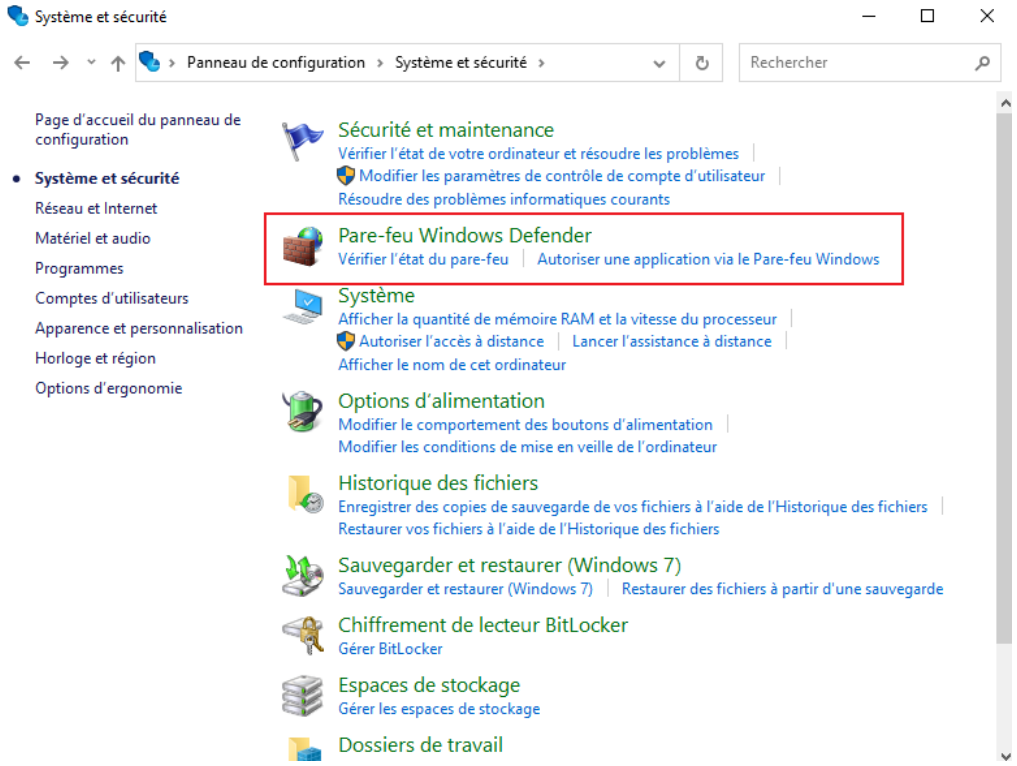
1 Qu'est-ce qu'un pare-feu ?

Un pare-feu est un programme logiciel ou un dispositif matériel qui contrôle le flux de contenu réseau depuis et vers l'ordinateur. Un pare-feu est généralement utilisé pour réduire ou empêcher le trafic Internet malveillant indésirable vers une adresse `IP` (l'adresse de l'ordinateur sur le réseau) en bloquant les ports utilisés par le trafic réseau.

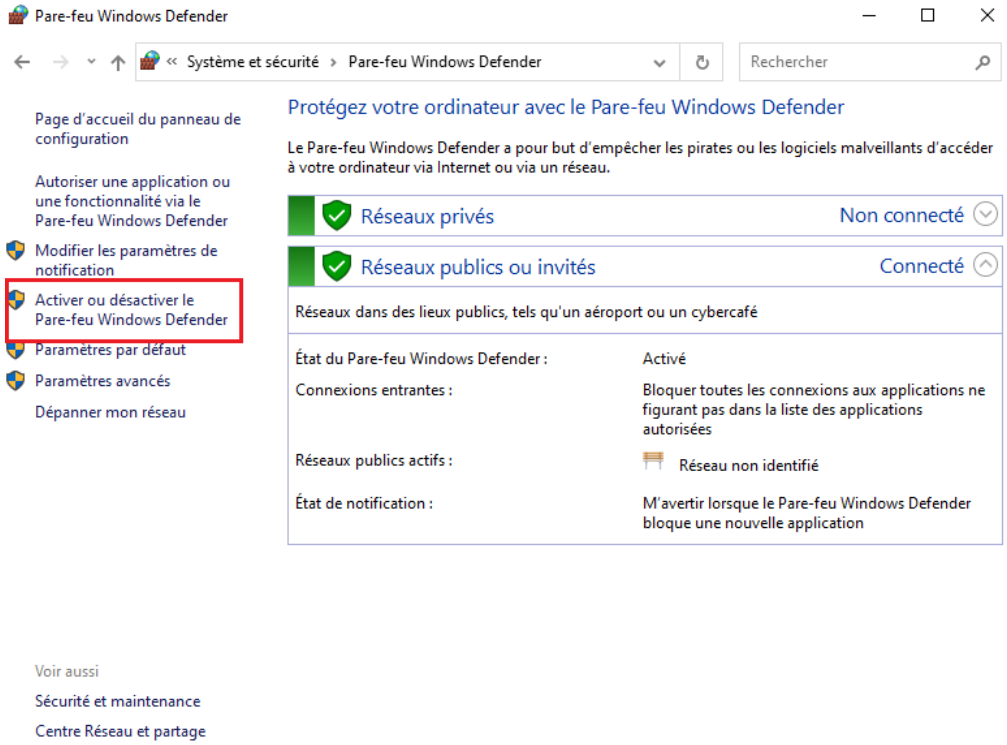
2 Activation ou désactivation du pare-feu Windows

Procédez comme suit pour activer ou désactiver le pare-feu Windows.

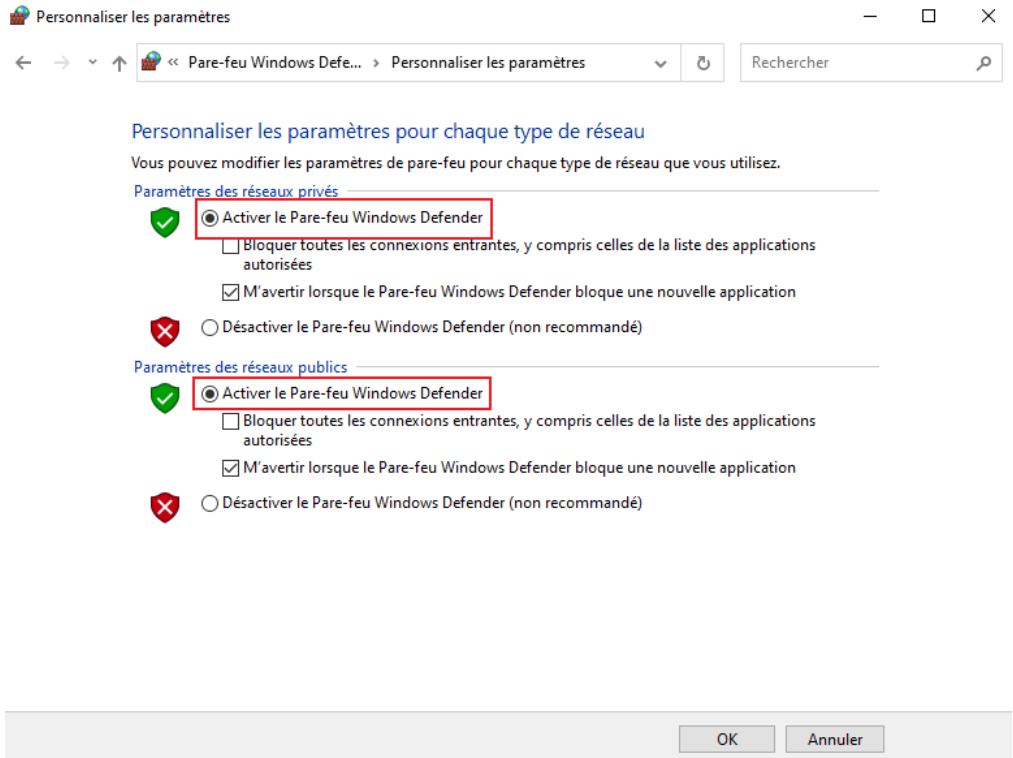
1. Pour activer le pare-feu *Windows*, cliquez sur **Démarrer**, **Panneau de configuration**, **Système et sécurité**, puis sur **Pare-feu Windows Defender**.



2. La page **Pare-feu Windows Defender** affiche les paramètres de pare-feu actuels. Pour activer le pare-feu, cliquez sur **Activer ou désactiver le pare-feu Windows Defender**.



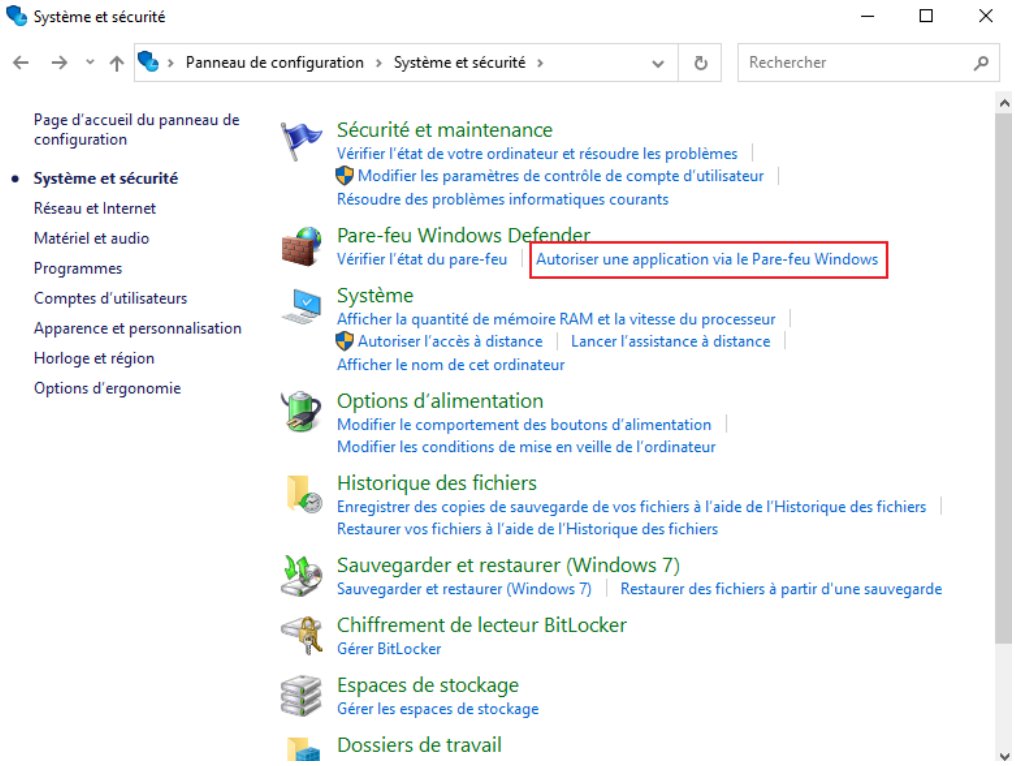
3. Sélectionnez **Activer le pare-feu Windows Defender** pour activer le pare-feu *Windows* afin de modifier les paramètres du pare-feu pour chaque type d'emplacement réseau que vous utilisez. Cliquez ensuite sur **OK**.



3 Autorisation des programmes par le biais du pare-feu

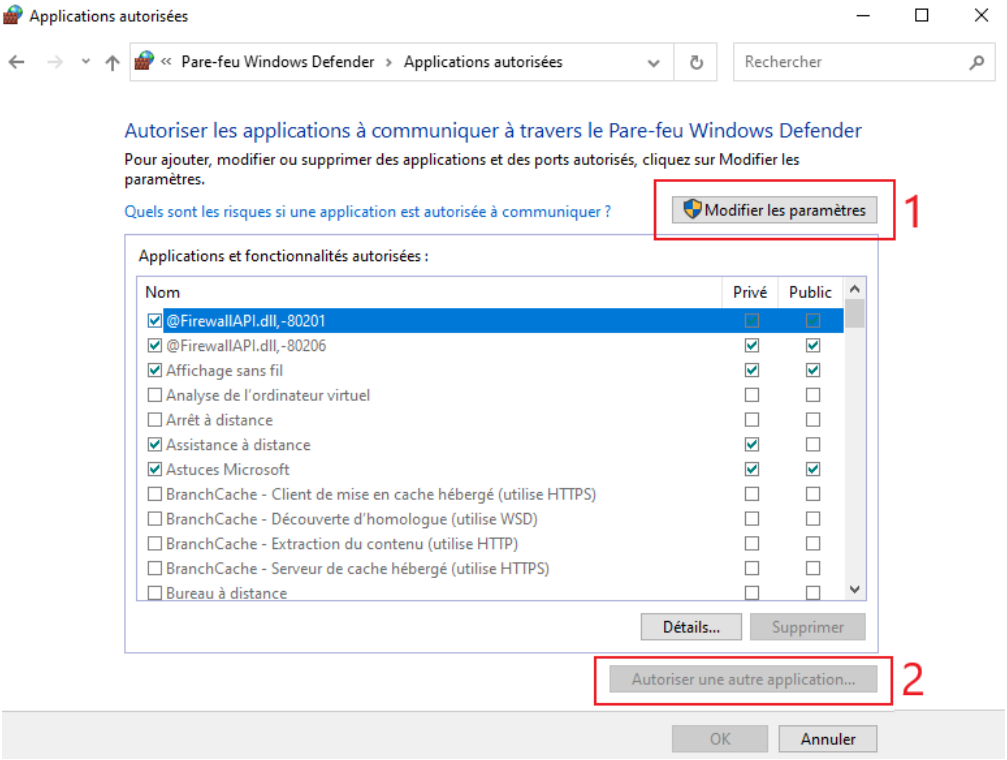
Si le logiciel de serveur est en cours d'utilisation en même temps que le pare-feu, le trafic Internet doit être en mesure d'accéder à ces serveurs par l'intermédiaire du pare-feu. Effectuez les étapes suivantes pour ouvrir le pare-feu pour **le logiciel de serveur** :

1. Pour autoriser des services via le pare-feu, cliquez sur **Démarrer**, **Panneau de configuration**, **Système et sécurité**, puis sur **Autoriser une application via le Pare-feu Windows**.



   Normalement, les programmes autorisés par le pare-feu *Windows* s'affichent.

2. Cliquez sur **Modifier les paramètres**. Cliquez ensuite sur **Autoriser une autre application...**.



3. Sélectionnez le programme que vous souhaitez ajouter ou cliquez sur **Parcourir** pour en trouver un qui n'est pas répertorié.
4. Cliquez sur **Ok** lorsque vous avez terminé.

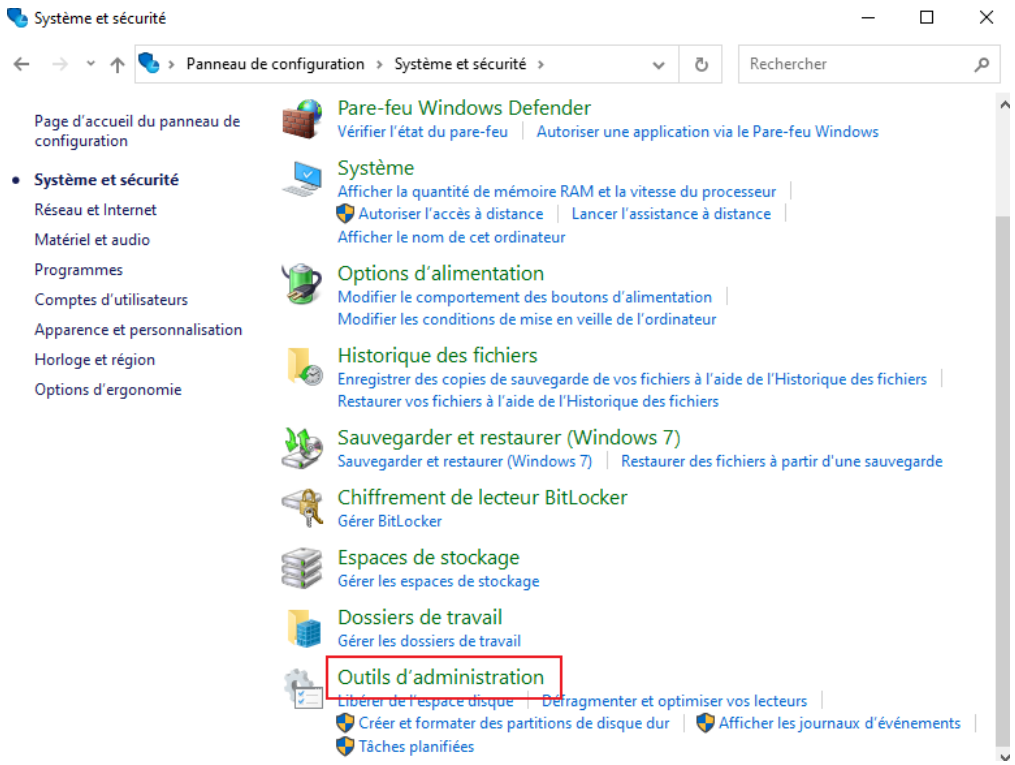
4 Contrôle du flux `ICMP` (*Internet Control Messaging Protocol*)

Certains messages envoyés par un autre ordinateur via Internet peuvent être reçus par un ordinateur. Par défaut, le logiciel de pare-feu *Windows* empêche l'envoi d'une réponse à ces messages. Cependant, vous pouvez activer la messagerie `ICMP` pour permettre à l'ordinateur de répondre aux demandes `ICMP`.

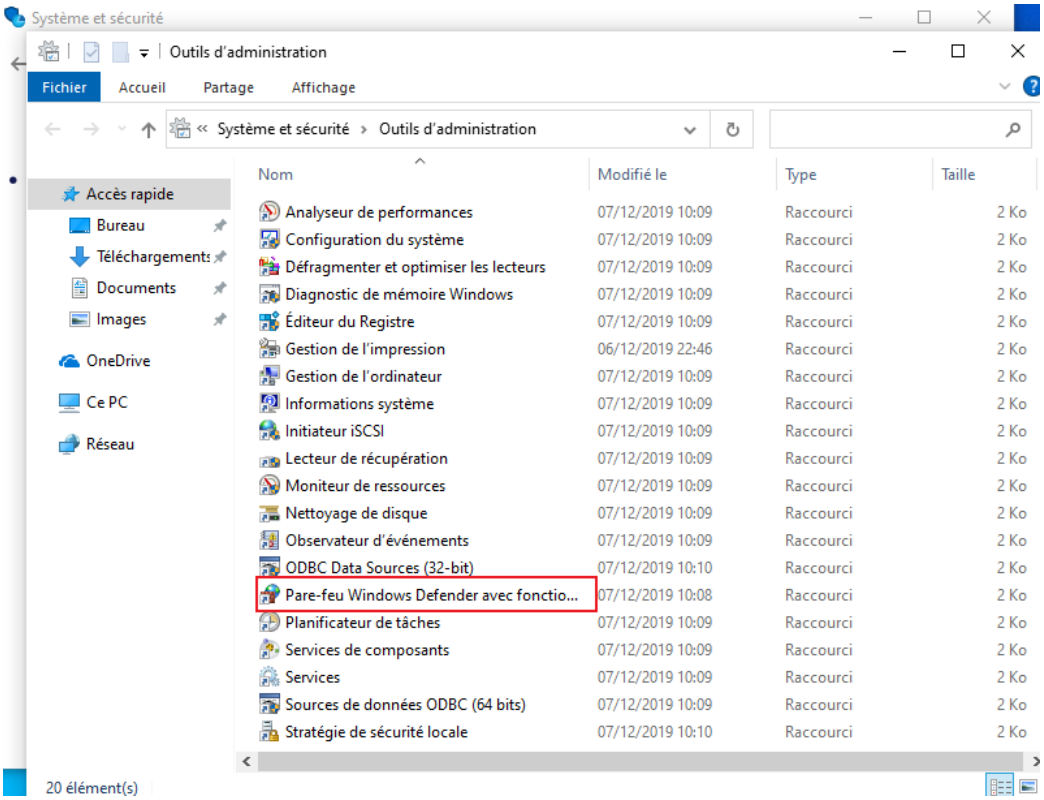
Ainsi, pour permettre à l'ordinateur de recevoir des demandes `ping` de dépannage, configurez une nouvelle règle pour permettre les demandes d'écho `ICMP`. Comme ceci peut rendre votre ordinateur vulnérable aux types d'attaques qui utilisent des messages d'écho `ICMP`, il est recommandé de désactiver cette règle dès que le dépannage est terminé.

Effectuez les étapes suivantes pour permettre à l'ordinateur de répondre aux messages `ICMP` :

1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**, **Sytème et sécurité**, puis faites défiler la liste et cliquez sur **Outils d'administration**.

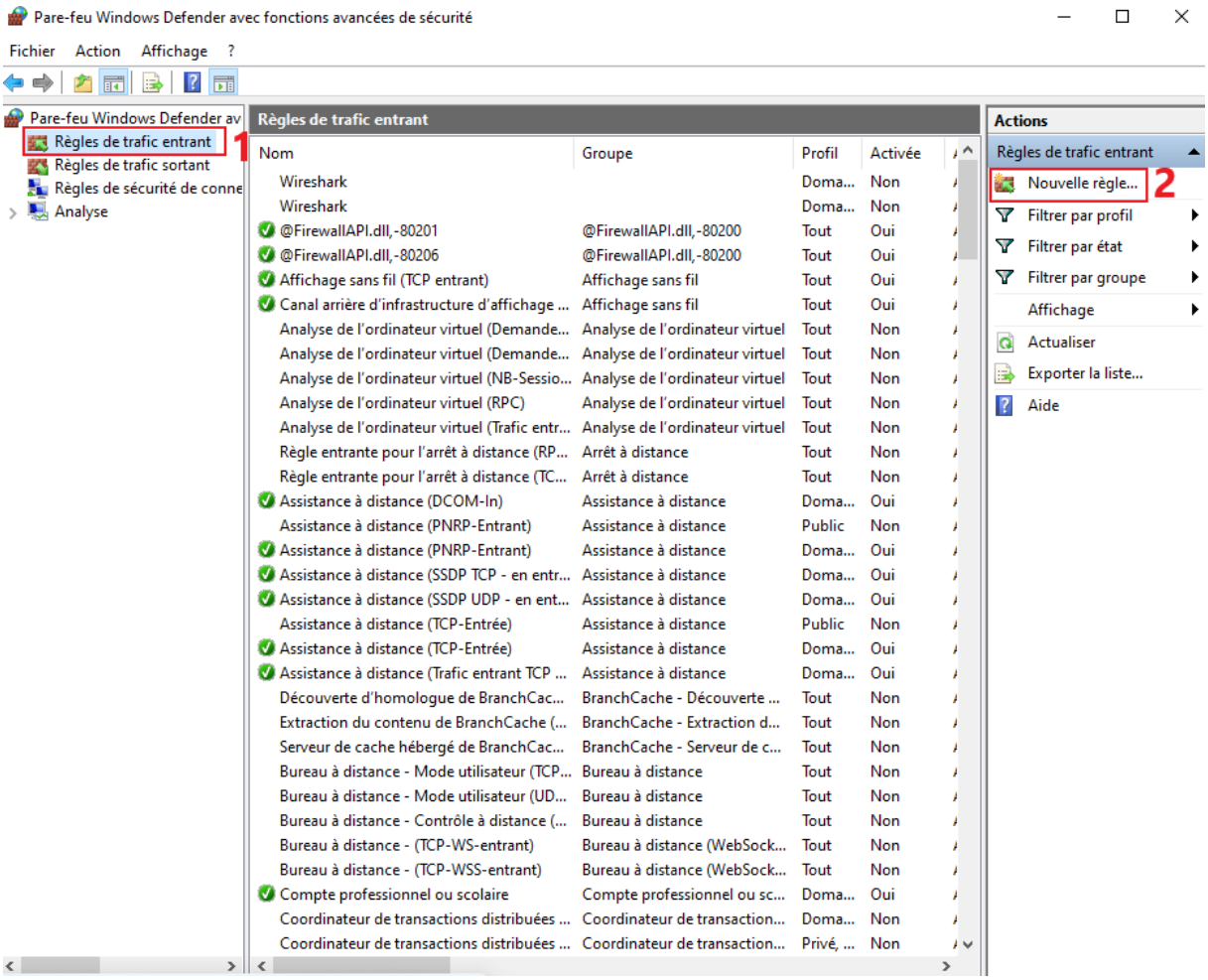


2. Double-cliquez sur **Pare-feu Windows Defender avec fonctions avancées de sécurité**.

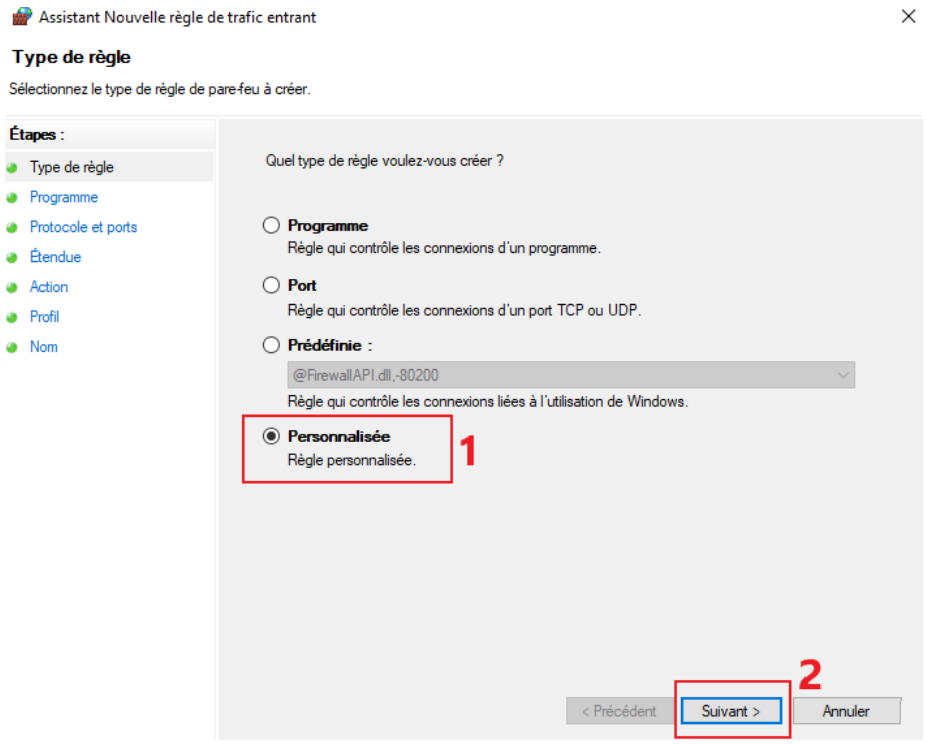


Normalement, **Pare-feu Windows Defender avec fonctions avancées de sécurité** s'ouvre.

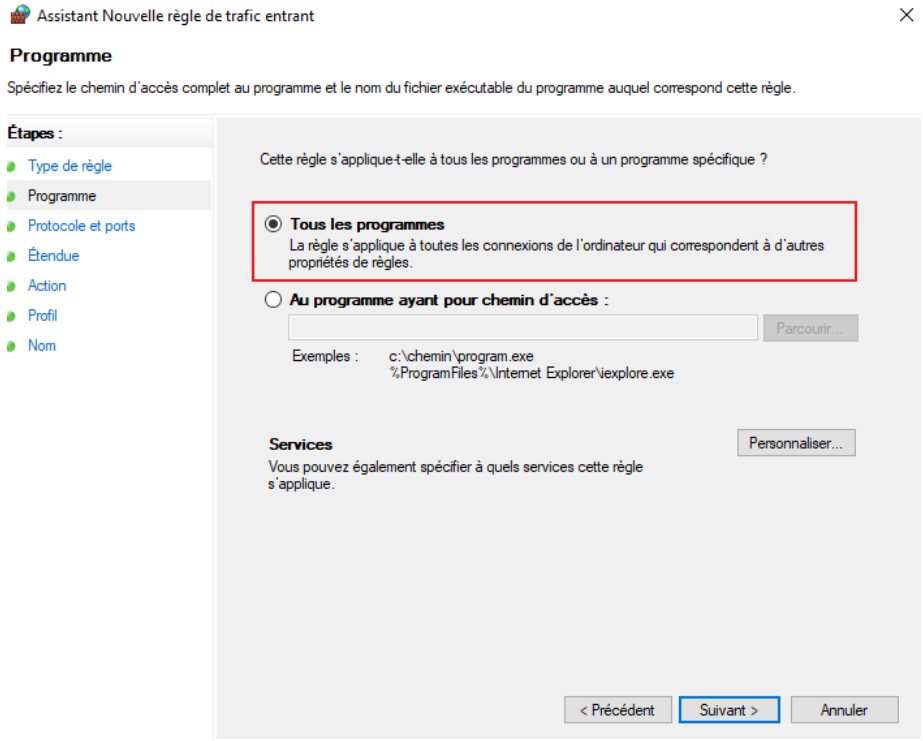
3. Cliquez sur **Règles de trafic entrant** dans le panneau de gauche. Dans le volet **Actions** situé sur la droite, cliquez sur **Nouvelle règle**.



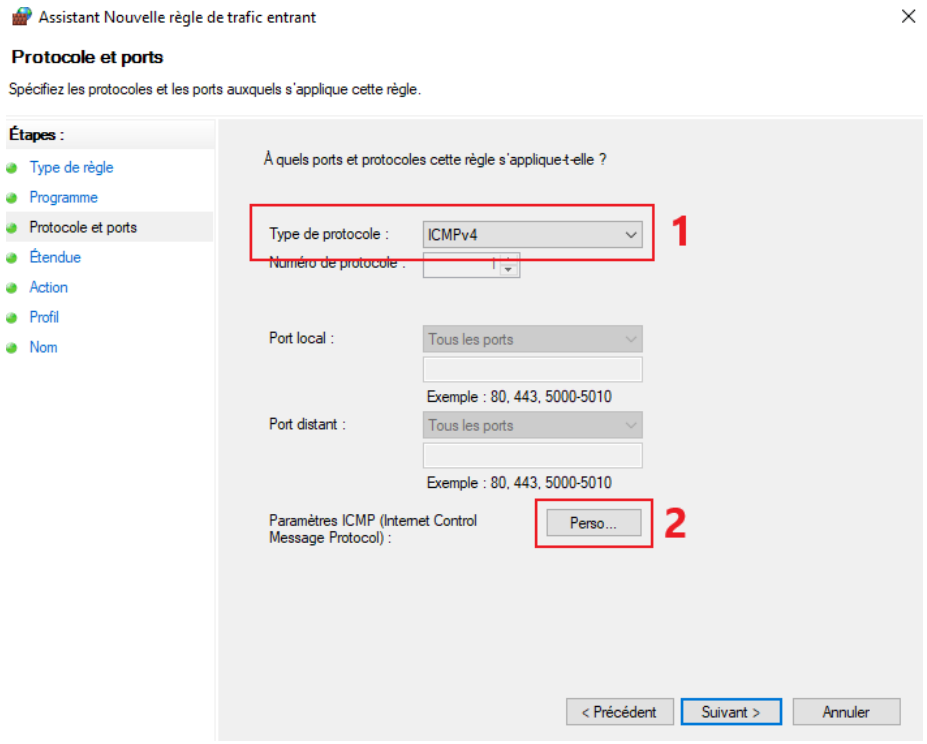
4. Sur la page Type de règle, cliquez sur **Personnalisée**, puis cliquez sur **Suivant**.



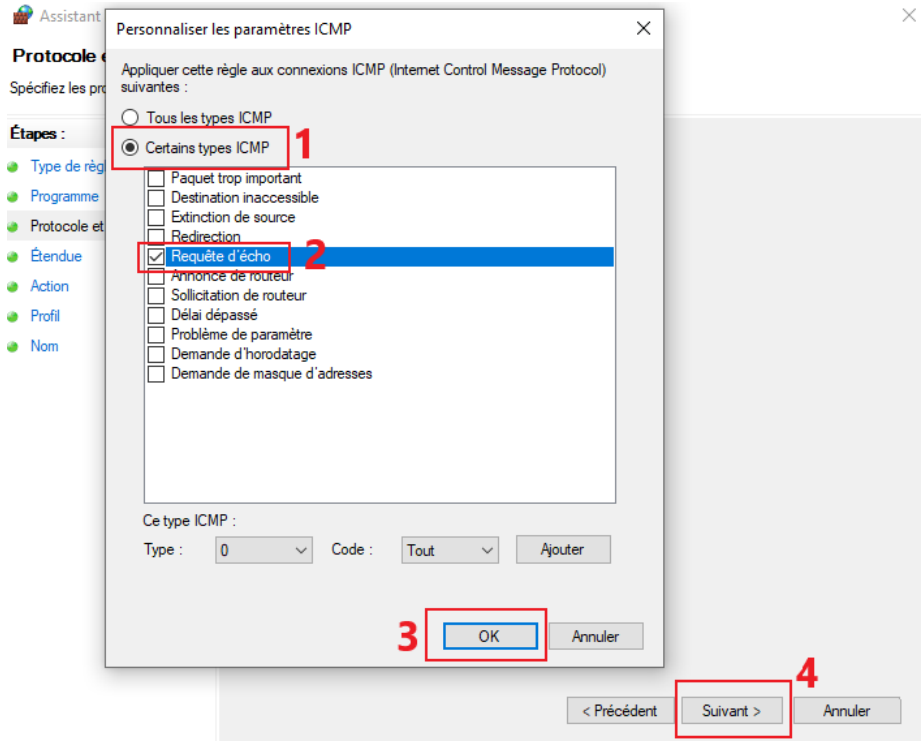
5. Sur la page Programme, cliquez sur **Tous les programmes**, puis sur **Suivant**.



6. Sur la page Protocole et ports, dans la zone **Type de protocole**, sélectionnez **ICMPv4**. Appuyez ensuite sur le bouton **Perso...**.



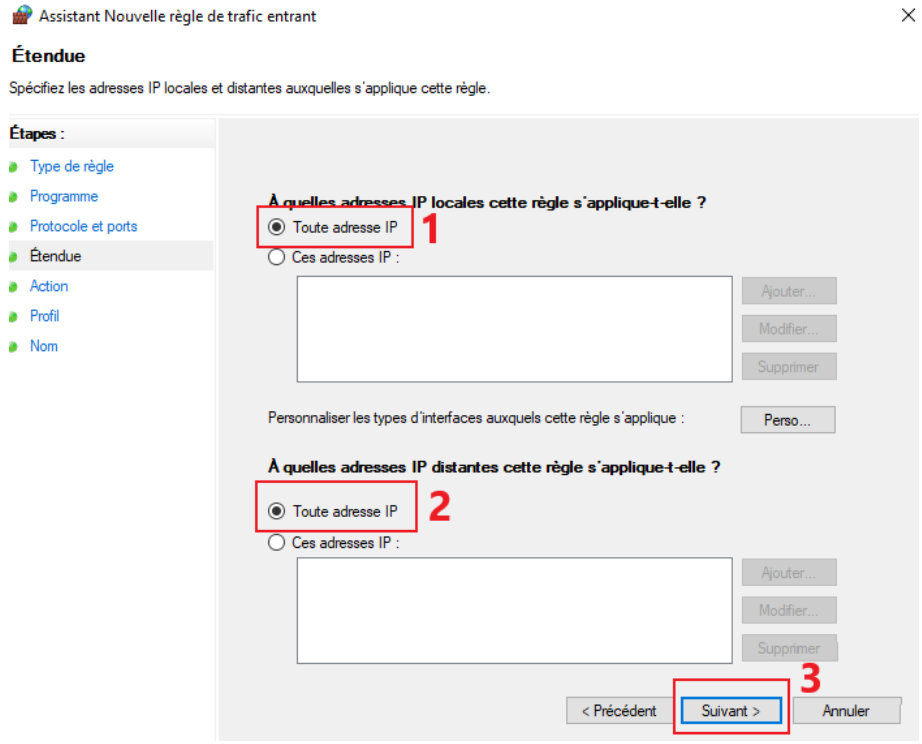
7. Sur la page Personnaliser les paramètres `ICMP`, cliquez sur **Certains types ICMP**. Sélectionnez ensuite le type `ICMP` spécifique à autoriser, tel que **Requête d'écho**. Cliquez sur **OK**, puis sur **Suivant**.



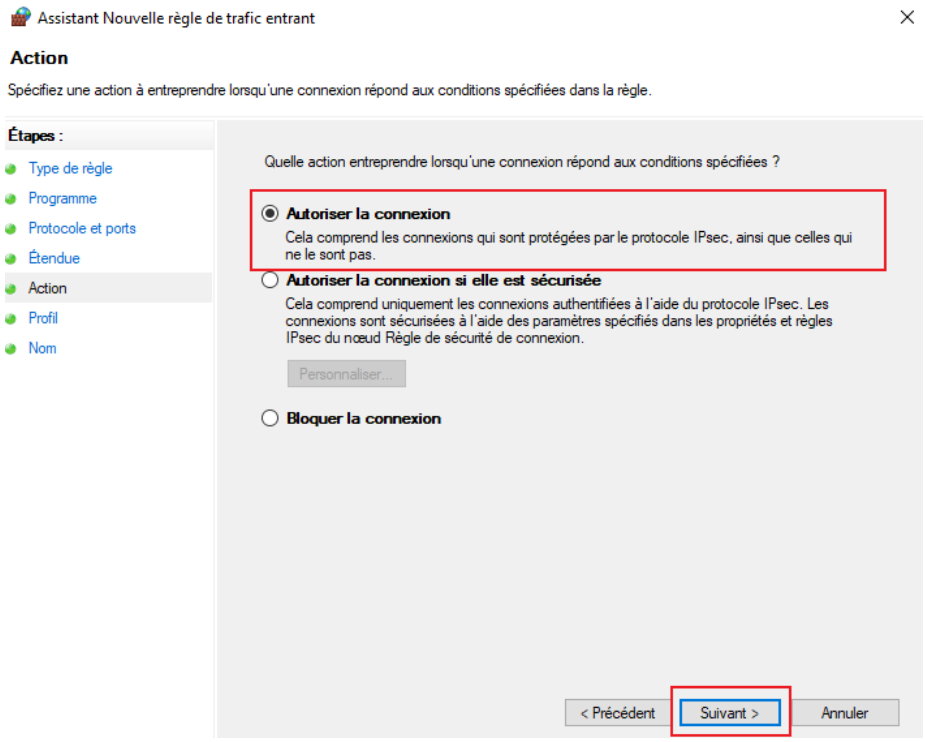
Consultez le tableau suivant pour obtenir davantage d'informations sur les éléments répertoriés.

Message ICMP	Fonction du message
Paquet trop important	Il s'agit d'un message indiquant que le paquet `IP` est trop important et qu'il doit être fragmenté pour pouvoir être envoyé au lien suivant dans la transmission.
Destination inaccessible	Réponse lorsque cet ordinateur ne peut pas résoudre une connexion pour un paquet d'informations.
Extinction de source	Lorsqu'il est impossible de maintenir la vitesse de transfert des données, ce message est renvoyé à l'expéditeur jusqu'à ce que la vitesse appropriée soit atteinte.
Rediriger	Il s'agit d'un message renvoyé par un autre périphérique réseau (en général un routeur) pour indiquer à l'ordinateur qu'il existe un meilleur chemin plus efficace vers l'adresse `IP` requise. L'autorisation de cet `ICMP` devrait permettre d'obtenir de meilleurs taux de transmission réseau.
Demande d'écho	Il s'agit de la commande `ping`. Ceci permet de vérifier la validité d'une adresse IP et de déterminer le temps nécessaire à l'envoi et à la réception de données. Les serveurs de jeu en réseau utilisent souvent cette commande sous une forme ou une autre.
Annonce de routage	Demande des routes utilisées par cet ordinateur pour aider au routage vers les dispositifs réseau voisins sur le même sous-réseau.
Sollicitation du routeur	Découverte/sélection/sollicitation du routeur pour aider les périphériques de réseaux voisins sur le même sous-réseau.
Délai dépassé	Il s'agit du message de retour indiquant à l'ordinateur expéditeur que le réassemblage d'un paquet prend trop longtemps.
Problème de paramètre	Il s'agit d'un message de réponse d'en-tête incorrect.
Demande d'horodatage	Cette requête permet de synchroniser les ordinateurs sur le réseau.
Demande de masque d'adresses	Demande des informations de masque de sous-réseau utilisées sur le réseau local lors de la mise sous tension d'un ordinateur.

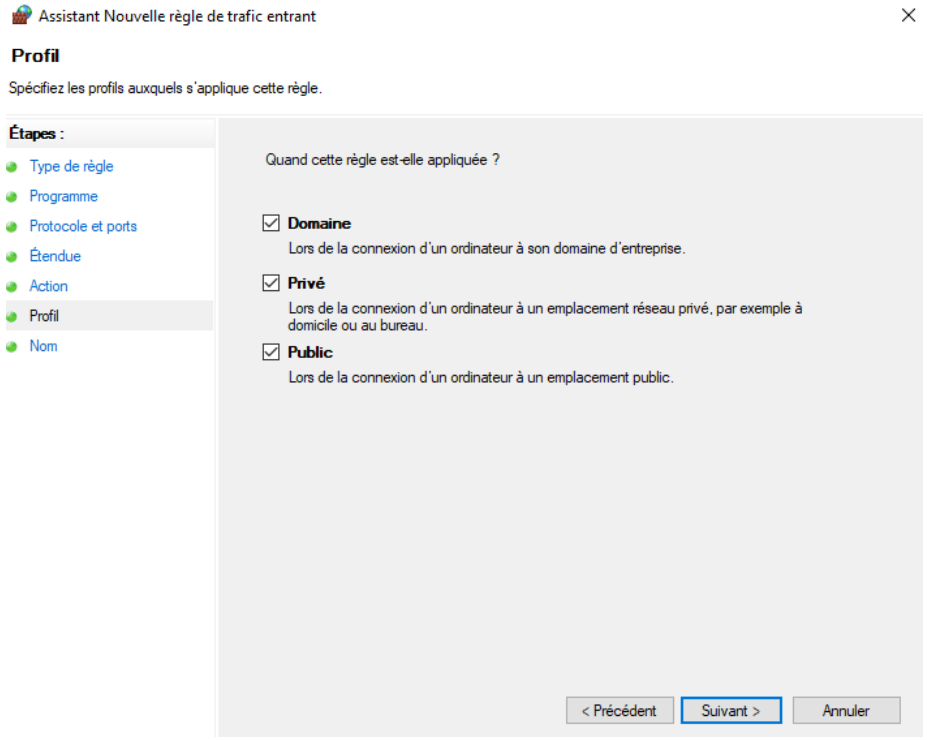
8. Sur la page Étendue, cliquez sur le réglage **Toute adresse IP** pour les adresses `IP` locales et distantes. Cliquez ensuite sur **Suivant**.



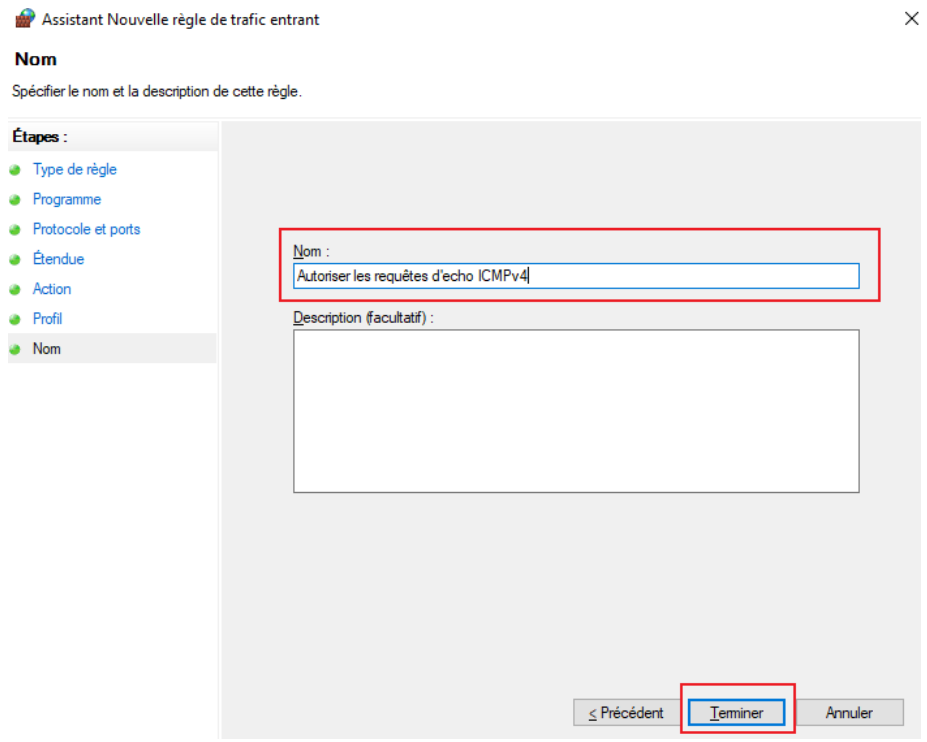
9. Sur la page Action, cliquez sur **Autoriser la connexion**, puis cliquez sur **Suivant**.



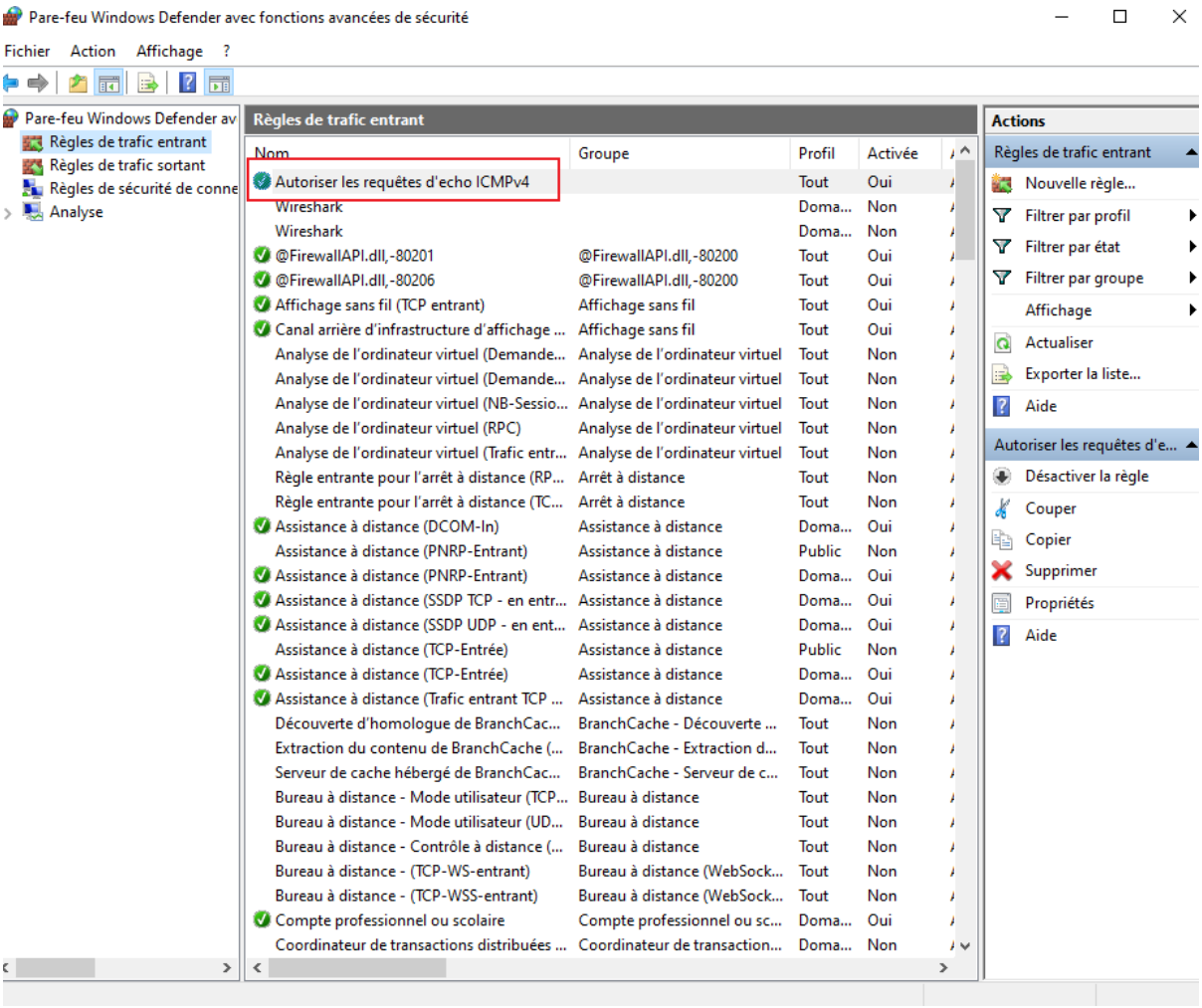
10. Sur la page Profil, sélectionnez les profils pour lesquels la règle s'applique, tels que **Domaine**, **Privé** et **Public**. Cliquez ensuite sur **Suivant**.



11. Sur la page Nom, tapez un **Nom** (obligatoire) et une **Description** (facultative) pour la règle. Cliquez ensuite sur **Terminer** pour revenir aux règles de trafic entrant.



On peut voir que notre règle a bien été ajoutée :


Pare-feu Windows Defender avec fonctions avancées de sécurité
Fichier Action Affichage ?
Pare-feu Windows Defender av
Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de conne
Analyse
Règles de trafic entrant
Nom Groupe Profil Activée
Autoriser les requêtes d'echo ICMPv4 Tout Oui
Wireshark Doma... Non
Wireshark Doma... Non
@FirewallAPI.dll,-80201 @FirewallAPI.dll,-80200 Tout Oui
@FirewallAPI.dll,-80206 @FirewallAPI.dll,-80200 Tout Oui
Affichage sans fil (TCP entrant) Affichage sans fil Tout Oui
Canal arrière d'infrastructure d'affichage ... Affichage sans fil Tout Oui
Analyse de l'ordinateur virtuel (Demande... Analyse de l'ordinateur virtuel Tout Non
Analyse de l'ordinateur virtuel (Demande... Analyse de l'ordinateur virtuel Tout Non
Analyse de l'ordinateur virtuel (NB-Sessio... Analyse de l'ordinateur virtuel Tout Non
Analyse de l'ordinateur virtuel (RPC) Analyse de l'ordinateur virtuel Tout Non
Analyse de l'ordinateur virtuel (Trafic entr... Analyse de l'ordinateur virtuel Tout Non
Règle entrante pour l'arrêt à distance (RP... Arrêt à distance Tout Non
Règle entrante pour l'arrêt à distance (TC... Arrêt à distance Tout Non
Assistance à distance (DCOM-In) Assistance à distance Doma... Oui
Assistance à distance (PNRP-Entrant) Assistance à distance Public Non
Assistance à distance (PNRP-Entrant) Assistance à distance Doma... Oui
Assistance à distance (SSDP TCP - en entr... Assistance à distance Doma... Oui
Assistance à distance (SSDP UDP - en ent... Assistance à distance Doma... Oui
Assistance à distance (TCP-Entrée) Assistance à distance Public Non
Assistance à distance (TCP-Entrée) Assistance à distance Doma... Oui
Assistance à distance (Trafic entrant TCP ... Assistance à distance Doma... Oui
Découverte d'homologue de BranchCac... BranchCache - Découverte ... Tout Non
Extraction du contenu de BranchCache (... BranchCache - Extraction d... Tout Non
Serveur de cache hébergé de BranchCac... BranchCache - Serveur de c... Tout Non
Bureau à distance - Mode utilisateur (TCP... Bureau à distance Tout Non
Bureau à distance - Mode utilisateur (UD... Bureau à distance Tout Non
Bureau à distance - Contrôle à distance (... Bureau à distance Tout Non
Bureau à distance - (TCP-WS-entrant) Bureau à distance (WebSock... Tout Non
Bureau à distance - (TCP-WSS-entrant) Bureau à distance (WebSock... Tout Non
Compte professionnel ou scolaire Compte professionnel ou sc... Doma... Oui
Coordinateur de transactions distribuées ... Coordinateur de transaction... Doma... Non
Actions
Règles de trafic entrant
Nouvelle règle...
Filtrer par profil
Filtrer par état
Filtrer par groupe
Affichage
Actualiser
Exporter la liste...
Aide
Autoriser les requêtes d'e...
Désactiver la règle
Couper
Copier
Supprimer
Propriétés
Aide

5 Dépannage du pare-feu *Windows*

Cette section traite des symptômes suivants :

— Le pare-feu *Windows* ne peut pas être activé ou désactivé dans le *Centre de sécurité*
— L'état du pare-feu n'est pas mis à jour dans le *Centre de sécurité*
— Le pare-feu est désactivé à chaque redémarrage de l'ordinateur

Pour résoudre la plupart des problèmes concernant le pare-feu *Windows*, réinitialisez le pare-feu en procédant comme suit :

1. Cliquez sur **Démarrer** et tapez **invite de commande** dans la zone Rechercher
2. Dans les résultats de la recherche, cliquez avec le **bouton droit de la souris** sur **Invite de commande**, puis cliquez sur **Exécuter en tant qu'administrateur**
3. Cliquez sur **Continuer** dans le message Contrôle de compte d'utilisateur
4. Dans la fenêtre d'**invite de commande**, saisissez la commande `netsh advfirewall reset`, puis appuyez sur **Entrée**

   Ceci réinitialise la configuration du pare-feu.