I'm not a bot

Le pare-feu Windows est un outil intégré qui vous aide à protéger votre ordinateur en surveillant les connexions entrantes et sortantes. Le problème, c'est qu'il peut aussi, parfois, être un peu trop restrictif et bloquer certaines applications que vous utilisez régulièrement. Pour en avoir le cœur net, voyons ensemble comment vérifier si le pare-feu empêche une application de fonctionner et comment résoudre ce problème en quelques clics. Avant de modifier quoi que ce soit dans les paramètres du pare-feu, certains signes peuvent vous indiquer que ce dernier bloque une application : Un message d'erreur dans l'application mentionnant un problème avec le pare-feu. Des difficultés à se connecter à Internet via l'application. Des fonctionnalités dépendant du réseau qui ne répondent pas. Des délais de connexion très longs, suivis d'une erreur. Et j'en passe… Si vous rencontrez un ou plusieurs de ces problèmes, il est possible que le pare-feu Windows en soit la cause. Pour vérifier si le pare-feu bloque une application, vous pouvez consulter la liste des applications autorisées dans les paramètres de Windows. Voici comment faire : Rendez-vous dans les paramètres de Windows (raccourci clavier : Win + I). Allez dans « Confidentialité et sécurité », puis dans « Sécurité Windows ». Cliquez sur « Ouvrir Sécurité Windows ». Dans « Sécurité Windows », choisissez « Pare-feu et protection du réseau ». Cliquez sur « Autoriser une application via le pare-feu ». La liste des applications autorisées ou bloquées s'affiche alors. Trouvez l'application concernée et vérifiez si les cases Privé et Public sont cochées. Si elles ne le sont pas, l'application est bloquée sur ce type de réseau. Pour autoriser une application bloquée : Cliquez sur « Modifier les paramètres » (vous devrez avoir les droits administratifs pour cela). Trouvez l'application dans la liste et cochez les cases « Privé » et/ou « Public » selon les réseaux sur lesquels vous voulez l'autoriser. Cliquez sur « OK » pour enregistrer vos changements. Cela permettra à l'application de fonctionner sans être bloquée par le pare-feu. Veillez toutefois à ne jamais autoriser une application non sécurisée, car cela peut mettre votre système en danger. Si votre application n'apparaît pas dans les applications autorisées, vous pouvez l'ajouter manuellement : Dans la fenêtre « Applications autorisées », cliquez sur « Ajouter une autre application ». Utilisez le bouton « Parcourir » pour sélectionner le fichier exécutable de l'application. Ajoutez-la à la liste et configurez ses permissions. Si l'application nécessite un port précis pour fonctionner et que celui-ci est bloqué, vous pouvez l'ouvrir manuellement : Dans « Pare-feu et protection du réseau », cliquez sur « Paramètres avancés ». La fenêtre « Pare-feu Windows Defender avec fonctions avancées de sécurité » s'ouvre. Cliquez sur « Règles de trafic entrant », puis sur « Nouvelle règle » dans le panneau de droite. Choisissez « Port », puis indiquez le numéro du port à ouvrir (par exemple, le port 443 pour HTTPS). Suivez les instructions à l'écran pour terminer la création de la règle. Ouvrez uniquement les ports nécessaires et uniquement pour des applications de confiance, afin de ne pas compromettre la sécurité de votre système. Chaque application que vous autorisez augmente le risque de compromission de votre système. Avant de donner l'autorisation, assurez-vous qu'il s'agit d'une source fiable et que vous en avez réellement besoin. Pour être encore plus sécurisé, pensez à activer le « Contrôle intelligent des applications » de Windows (si disponible). Ce dernier vous aidera à analyser les applications installées et celles que vous prévoyez d'utiliser, vous apportant une sécurité supplémentaire. Et n'oubliez pas de toujours garder votre système et vos outils de sécurité à jour. Le pare-feu Windows est un outil puissant qui protège vos données, mais il peut parfois poser problème pour certaines applications. En suivant ces étapes, vous pourrez identifier et ajuster facilement les réglages pour rétablir leur bon fonctionnement. Cependant, gardez bien en tête de vérifier la fiabilité des logiciels avant de modifier les permissions du pare-feu. Les logiciels ont parfois besoin d'échanger des informations via le réseau. Cette action est requise lorsqu'une application doit transmettre des données à d'autres appareils connectés au même réseau. Généralement, les applications signalent cette nécessité et sollicitent votre accord pour communiquer via le réseau lors de leur installation ou de leur premier lancement. Si vous désirez autoriser ou interdire à une application l'accès au réseau, cela s'effectue à travers les paramètres du pare-feu. Voici comment procéder. Gérer l'accès au réseau Ouvrez le Panneau de configuration et naviguez vers la section Système et sécurité. Ensuite, sélectionnez Pare-feu Windows Defender. Vous pouvez également accéder directement en ouvrant l'Explorateur de fichiers et en collant le chemin suivant dans la barre d'adresse, puis en validant avec Entrée. Cliquez ensuite sur « Pare-feu Windows Defender » dans la fenêtre apparue. Control PanelSystem and Security Dans la fenêtre qui s'affiche, cliquez sur l'option « Autoriser une application ou une fonctionnalité via le pare-feu Windows » située dans la colonne de gauche. Dans la fenêtre suivante, appuyez sur le bouton « Modifier les paramètres ». Des droits d'administrateur seront nécessaires pour modifier les configurations du pare-feu. Après avoir cliqué sur « Modifier les paramètres », les options de contrôle sous « Applications et fonctionnalités autorisées » deviennent modifiables. Parcourez la liste des applications et cochez les cases « Privé » ou « Public » pour donner à l'application le droit de communiquer sur les réseaux privés et publics. Inversement, vous pouvez désactiver une case pour interdire à une application l'accès au réseau. Si une application spécifique ne figure pas dans la liste, faites défiler jusqu'en bas et cliquez sur le bouton « Autoriser une autre application » afin de la sélectionner et de lui accorder l'accès au réseau. Mise en garde importante Sauf nécessité absolue, il est déconseillé d'autoriser une application à communiquer avec d'autres ordinateurs sur le réseau. Les applications nécessitant cet accès pour fonctionner demanderont votre autorisation lors de leur exécution ou de leur installation. Dans tous les cas, l'application doit provenir d'un développeur de confiance et être téléchargée depuis une source fiable. Par exemple, si vous téléchargez VLC, assurez-vous de le faire depuis le site web officiel et non à partir d'un dépôt de logiciels ou d'un lien de stockage cloud d'une tierce personne. Il est judicieux de vérifier régulièrement cette liste et d'examiner quelles applications sont autorisées à échanger des données via le réseau. Si vous identifiez des applications que vous n'utilisez pas fréquemment ou dont vous ne vous souvenez pas de l'installation, envisagez de leur révoquer l'accès au réseau (voire de les désinstaller). Souhaitez-vous bloquer l'accès Internet d'une application ? Vous pouvez configurer une règle spécifique dans le pare-feu Windows.