



Test de Comodo Firewall : pare-feu, HIPS, sandbox et plus encore !



2 votes



TEST FIREWALL COMODO

Le 9 mars 2017 • 3 vues • [0 commentaire](#)

Page 4 : Test de Comodo Firewall : pare-feu, HIPS, sandbox et plus encore !

L'éditeur **Comodo** propose de nombreux **logiciels de sécurité** (Firewall, Antivirus, TrustConnect Wifi Security et BOClean Anti-Malware) réunis autour d'un seul et même programme : **Internet Security**. La particularité de cette suite de sécurité est qu'elle est **entièrement gratuite** ! C'est assez surprenant mais c'est bien le cas : Comodo propose effectivement une **suite de sécurité comprenant un antivirus, un pare-feu** et tout un tas d'outils de sécurité **gratuitement**.

Comodo Internet Security existe dans des versions Pro et Entreprise avec, pour la **version Pro**, un support produit illimité, une téléassistance illimitée pour la suppression de virus et 500\$ de garantie sans aucun virus ; pour la **version Entreprise**, les mêmes options que la version Pro + 50 Go d'espace de stockage en ligne et 10 Go pour le logiciel TrustConnect WiFi Security. Autant dire que la **version Free** est largement suffisante pour la plupart des

utilisateurs. Bien que ce Comodo Internet Security semble très complet, dans le cadre de ce [comparatif sur les pare-feux Windows](#), nous voudrions juste installer le **module Firewall de Comodo**. Heureusement, c'est possible ! Tout comme l'antivirus, il est possible d'installer le **pare-feu de Comodo seul**, sans tout l'attirail de la suite de sécurité.

Pare-feu réputé pour ses qualités depuis plusieurs années, **Comodo Firewall** est-il à la hauteur de sa réputation ?

AU SOMMAIRE

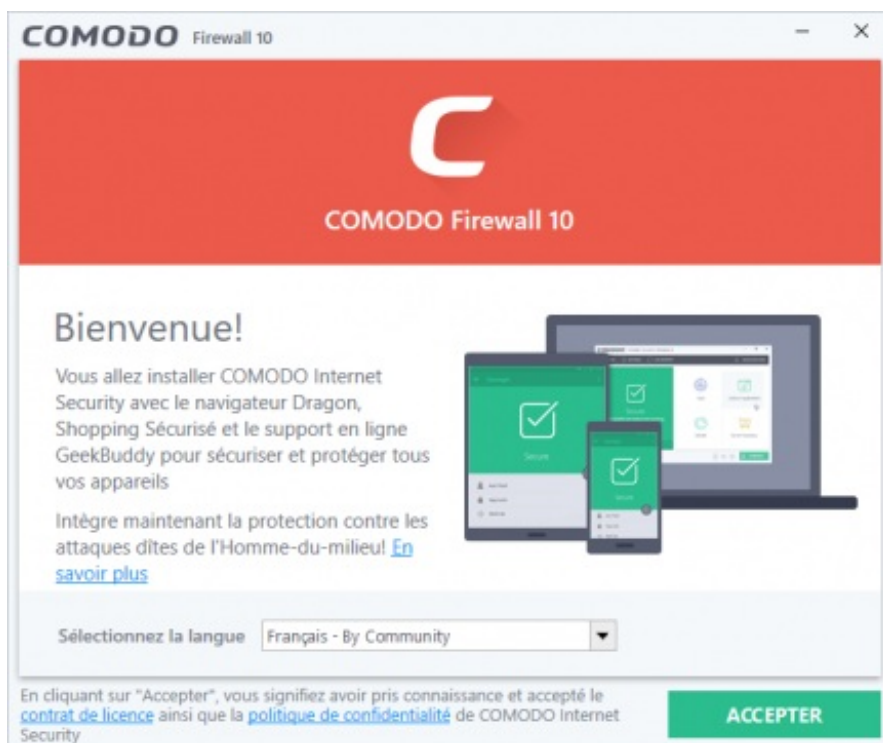
1. [Installation](#)
2. [Fonctionnalités](#)
 - 2.1. [Pare-feu](#)
 - 2.2. [HIPS](#)
 - 2.3. [Auto-sandbox](#)
 - 2.4. [Autres fonctionnalités](#)
3. [Verdict de Comodo Firewall](#)

Installation

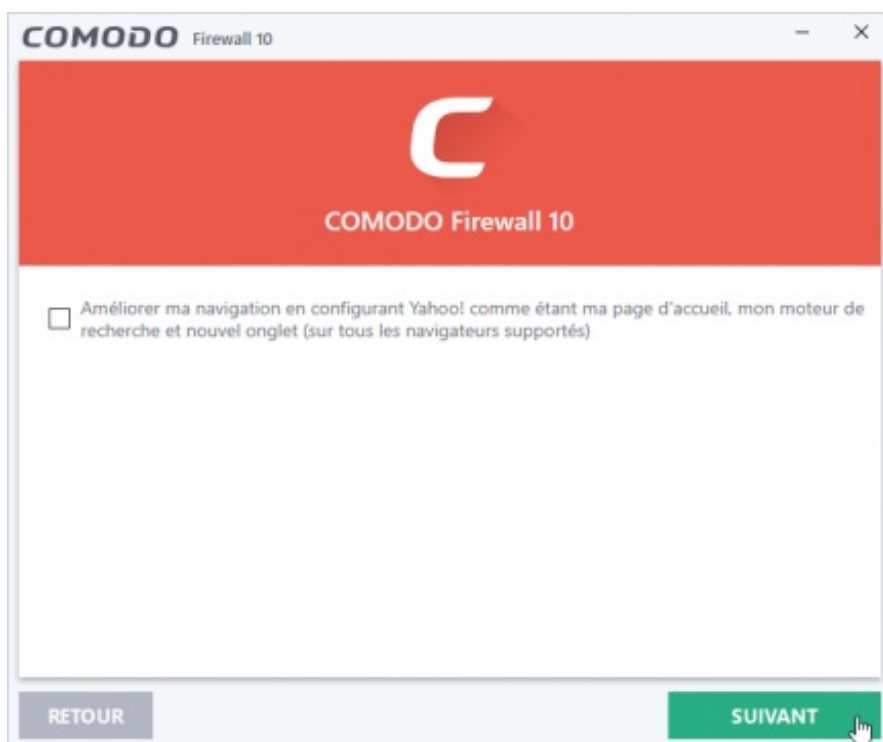
Comme je l'ai dit en introduction, le cœur même de Comodo est son logiciel **Internet Security** qui regroupe toutes les applications de sécurité de l'éditeur. Il est heureusement possible d'installer la plupart de ces applications à part. Vous trouvez ci-après le lien pour télécharger uniquement l'application pare-feu : **Comodo Firewall**.

[Télécharger Comodo Firewall](#)

Après l'avoir téléchargé, lancez l'exécutable du programme d'installation de **Comodo Firewall**.



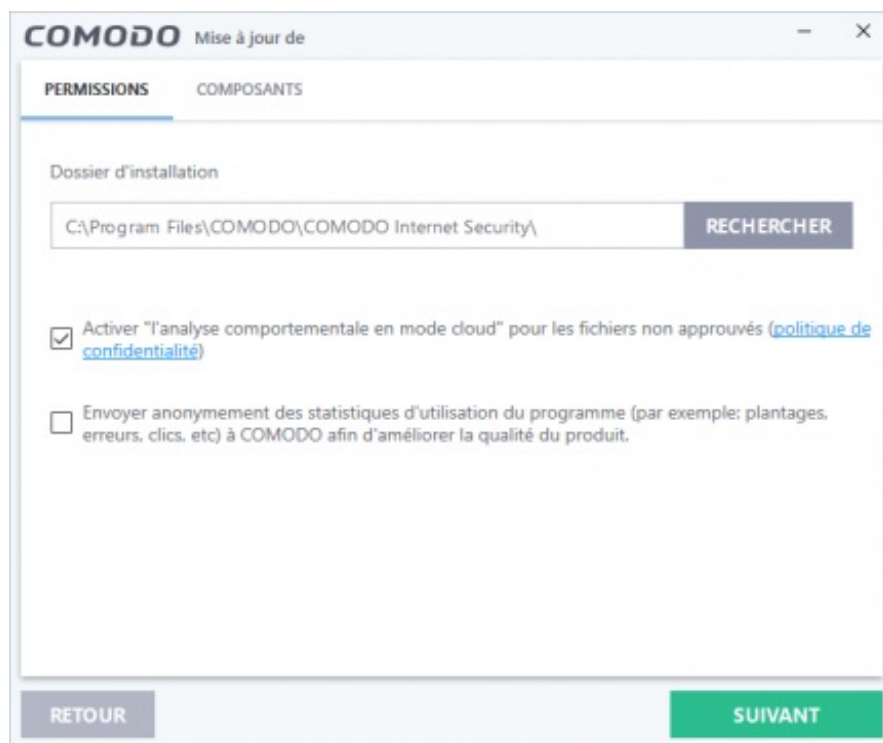
Décochez la case pour la configuration de Yahoo! comme page d'accueil et moteur de recherche par défaut sur votre navigateur Internet puis cliquez sur **Suivant**.



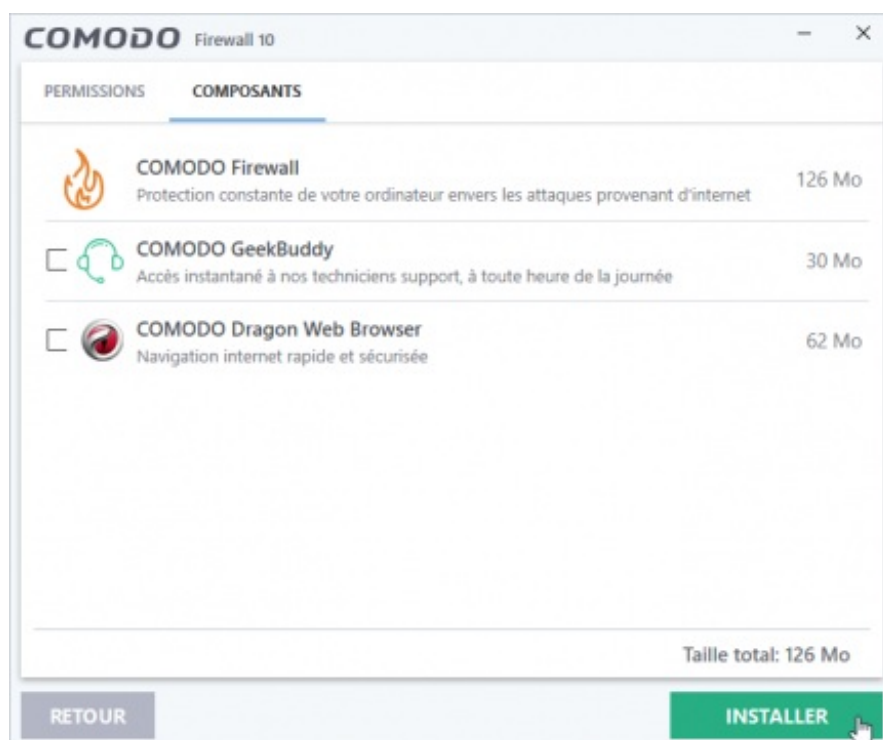
Dans l'onglet **Permissions**, vous pouvez choisir ou non d'activer l'**analyse comportementale en mode cloud** pour les fichiers non approuvés. Chaque fichier identifié comme inconnu sera envoyé au serveur Comodo Instant Malware Analysis (CIMA) pour une **analyse comportementale** : le fichier est exécuté dans un environnement virtuel sur les serveurs de Comodo et testé pour déterminer s'il se comporte de **manière malveillante**. Si c'est le cas, le fichier est envoyé aux techniciens de chez Comodo pour une analyse manuelle pour confirmer ou infirmer la malveillance du fichier. Les résultats sont ensuite envoyés à votre ordinateur

dans les 15 minutes. Il est recommandé de laisser cette **option activée**.

Pour ce qui est de l'**envoi des statistiques** d'utilisation du programme, c'est vous qui voyez !

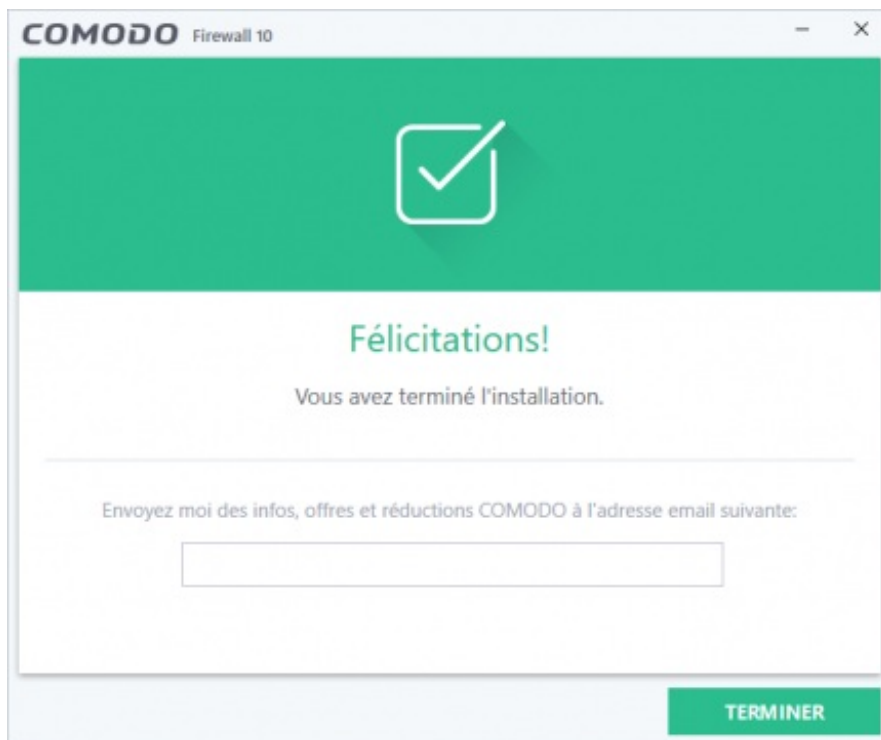


Dans l'onglet **Composants**, vous avez la possibilité d'installer le navigateur **Comodo Dragon Web Browser**. Celui-ci est loin d'être indispensable. Quant à **Comodo GeekBuddy**, il est réservé aux utilisateurs qui ont une version Pro ou Complete de Comodo Internet Security. Décochez donc ces deux cases puis cliquez sur le bouton **Installer** pour lancer l'installation de **Comodo Firewall**.

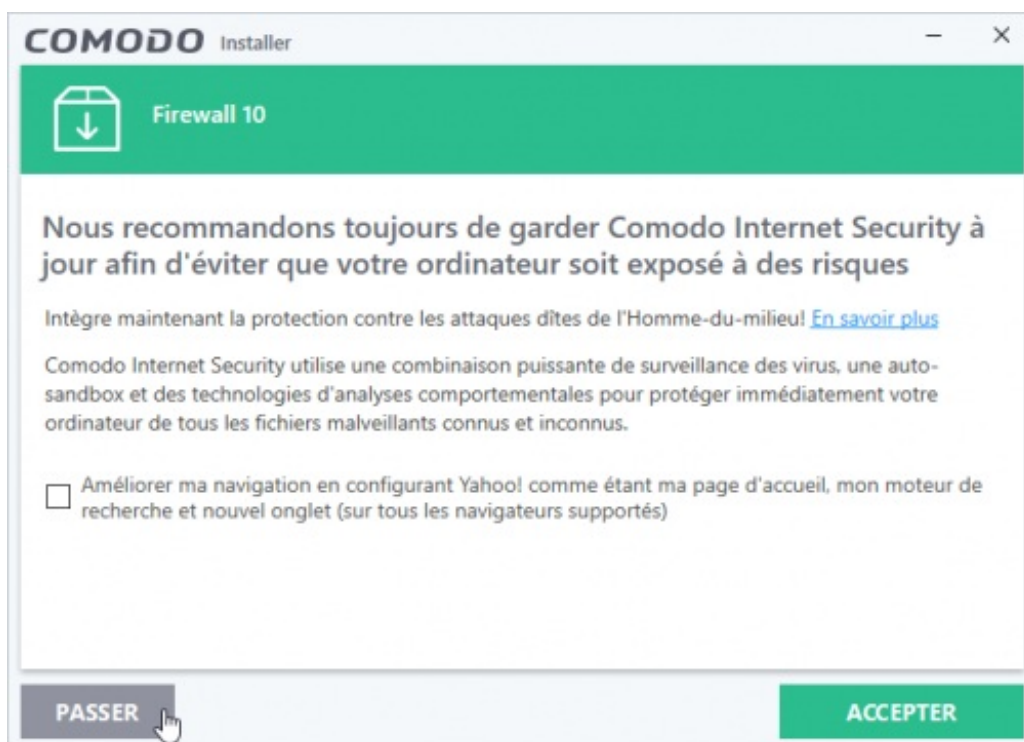


Une fois l'installation terminée, cliquez sur le bouton **Terminer** et redémarrez votre PC pour

que **Comodo Firewall** se lance en même temps que Windows.



Après le redémarrage, vous serez invité une seconde et dernière fois à installer Yahoo! sur votre système. Décochez la case et cliquez sur le bouton **Passer**.



Même s'il est un peu lourd à nous « proposer » l'installation Yahoo!, on comprend a besoin de gagner de l'argent quelque part, surtout quand on propose une solution de sécurité gratuite.

Maintenant, allons voir ce que ce **Comodo Firewall** a dans le ventre !

Fonctionnalités

Bien que gratuit, les fonctionnalités proposées par **Comodo Firewall** sont nombreuses et alléchantes :

- **Pare-feu** : 4 modes de fonctionnement (bloquer tout, personnalisé, sécurisé et apprentissage), option pour cacher les ports du PC et voir toutes les connexions en cours.
- **Système Host Intrusion Protection (HIPS)** : surveille constamment toutes les applications et tous les exécutables du système. HIPS un outil efficace contre les programmes malveillants (rootkits, keyloggers...) qui tentent de modifier les paramètres du système car toute action jugée suspecte sera soumise à l'approbation de l'utilisateur.
- **Analyse comportementale basée sur le cloud** : analyse les fichiers non reconnus dans le cloud. Tout fichier qui n'est pas reconnu et qui ne figure pas dans la liste blanche de Comodo est envoyé au serveur CIMA (Comodo Instant Malware Analysis) pour une analyse de comportement.
- **Auto-sandbox** : exécute automatiquement les programmes inconnus dans un environnement sécurisé isolé du reste de votre ordinateur (sandbox ou « bac au sable »).
- **Bureau virtuel** : environnement virtuel dans lequel l'utilisateur peut exécuter des programmes et visiter des sites Web dans lesquels il n'a pas confiance à 100%.
- **Viruscope** : surveille l'activité des processus en cours d'exécution et alerte si les actions d'une application pourraient potentiellement menacer la vie privée et/ou la sécurité de l'utilisateur. Il est possible de bloquer les actions potentiellement indésirables du logiciel sans pour autant bloquer le logiciel entièrement.

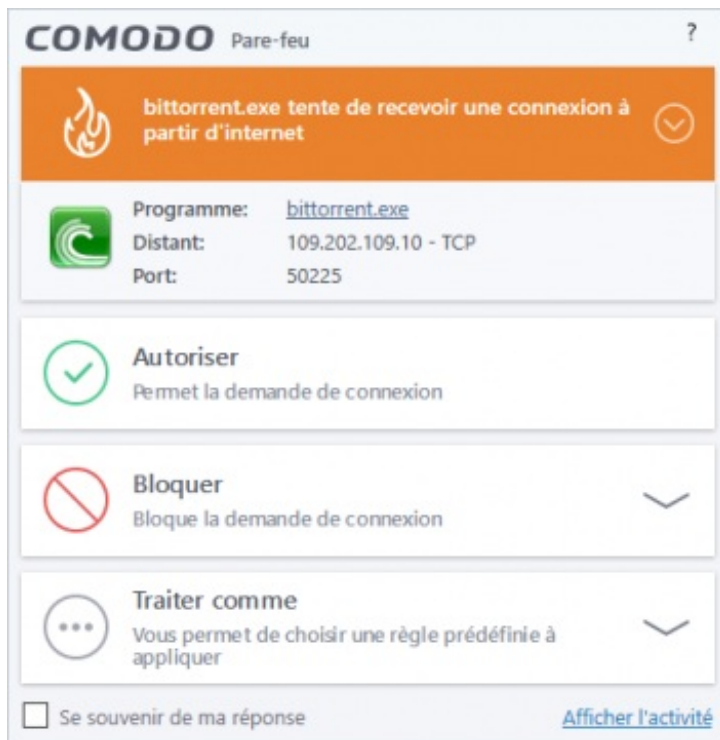
Pour un logiciel gratuit, on ne peut que se réjouir de toutes les fonctionnalités proposées par ce **Comodo Firewall** ! Faisons maintenant un petit tour d'horizon de chacune de ces fonctionnalités.

Pare-feu

Le pare-feu de Comodo peut fonctionner en 4 modes différents :

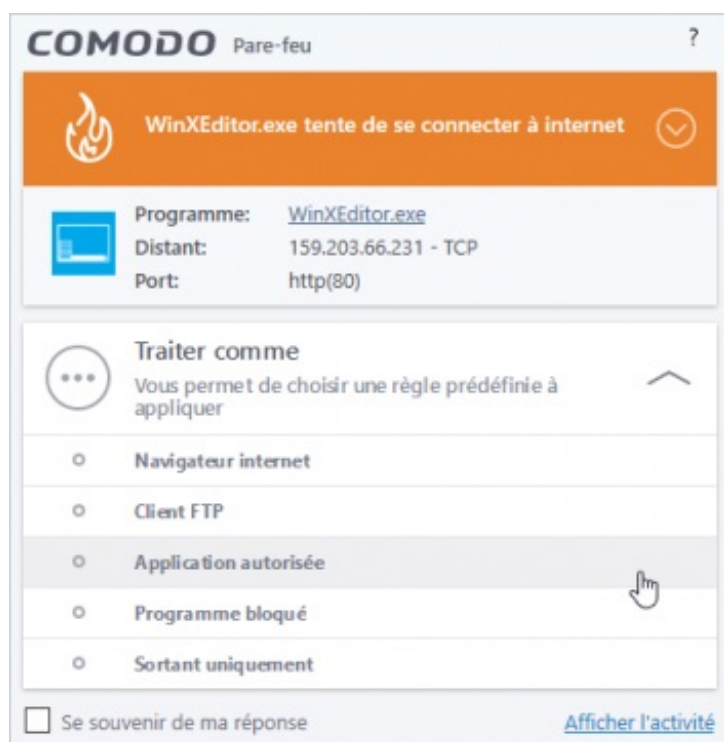
- **Bloquer tout** : le pare-feu bloque tout le trafic entrant et sortant de l'ordinateur, peu importe la configuration et les règles définies par l'utilisateur. Le pare-feu ne tente pas d'apprendre le comportement d'une application et ne crée pas automatiquement de règles de trafic pour les applications. Cette option **empêche l'ordinateur d'accéder à tous les réseaux**, y compris Internet.

- **Mode personnalisé** : le pare-feu applique **uniquement** les paramètres de sécurité et les règles de trafic spécifiés par l'utilisateur. On peut voir ce mode comme un mode « Ne pas apprendre » car le pare-feu ne tentera pas d'apprendre le comportement des applications ; il ne créera pas non plus automatiquement des règles de trafic réseau pour ces applications. Vous recevrez des alertes à **chaque tentative de connexion d'une application** (sauf si bien sûr vous avez déjà définis des règles personnalisées pour cette application). Ce mode est conseillé pour les **utilisateurs avancés** qui souhaitent avoir une visibilité et un contrôle maximales du trafic entrant et sortant de leur ordinateur.



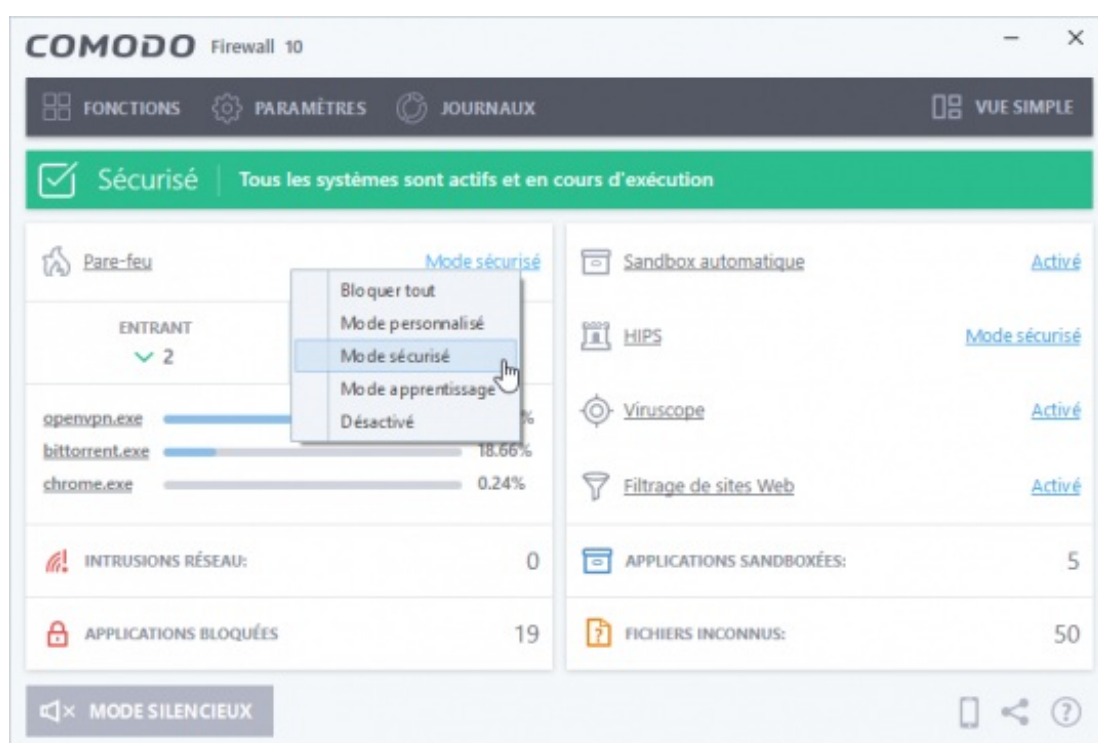
Alerte de pare-feu pour une tentative de connexion entrante de l'application BitTorrent (mode personnalisé)

- **Mode sécurisé (par défaut)** : le pare-feu crée **automatiquement** des règles qui autorisent tout le trafic pour les **applications certifiées « saines »** par Comodo (si l'option *Créer des règles pour des applications saines* est cochée). Pour les applications non certifiées, vous recevrez une alerte chaque fois qu'une de ces applications tente d'accéder au réseau : vous pourrez alors choisir de refuser ou d'accorder l'accès Internet à une application en choisissant par exemple *Traiter comme une application autorisée* sur l'alerte Comodo. Cela appliquera la règle prédéfinie « Application autorisée » sur l'application (nous verrons l'intérêt des **règles prédéfinies** tout à l'heure). Le mode sécurisé est le **paramètre recommandé pour la plupart des utilisateurs**, le niveau de sécurité est élevé et le nombre d'alertes de connexion facile à gérer.

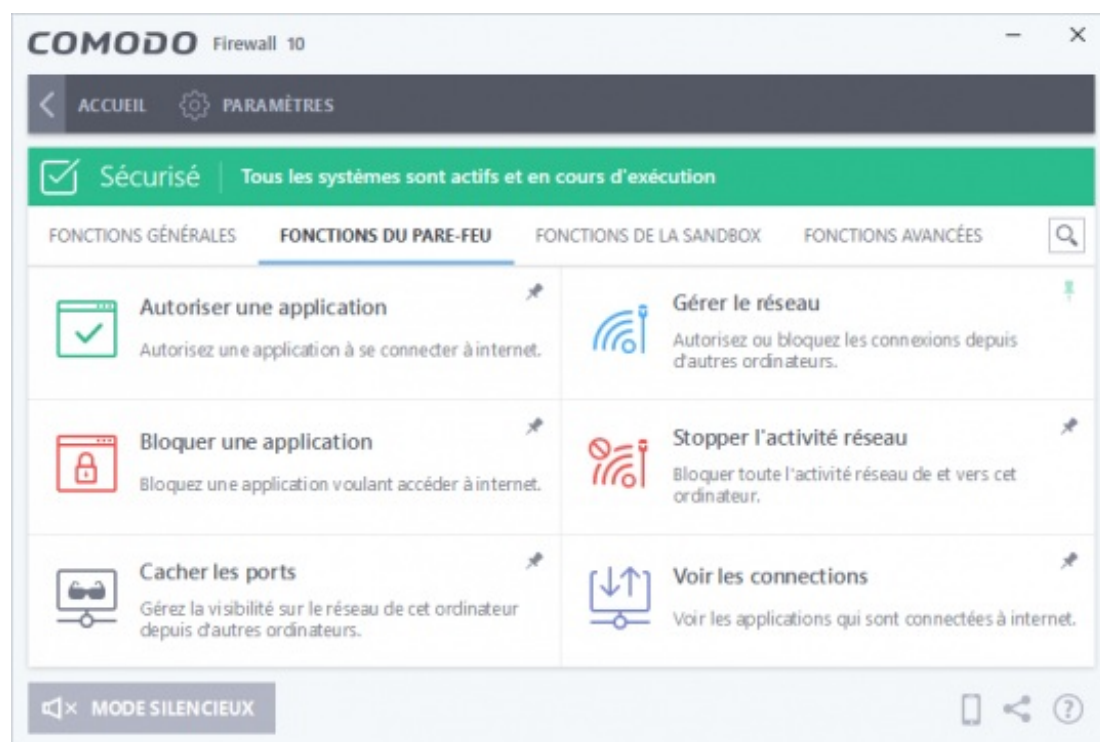


Alerte de pare-feu pour une tentative de connexion sortante d'une application non approuvée (mode sécurisé)

- Mode apprentissage** : le pare-feu surveille le trafic réseau et crée automatiquement des règles « Autoriser » pour toutes les nouvelles applications qui demande l'accès au réseau. Vous ne recevrez aucune alerte dans ce mode apprentissage. A utiliser en cas de nécessité absolue ! Ce mode peut-être utile pour les jeux vidéo qui requièrent l'accès au réseau : activez le mode apprentissage, lancez votre jeu, jouez pendant 2-3 minutes le temps que Comodo crée les règles d'autorisation nécessaires pour le jeu vidéo puis revenez à un mode plus sûr. Soyez sûr à 100% que toutes les applications installées sur votre ordinateur disposent de règles d'accès appropriées avant de lancer ce mode.



Outre les classiques options **Autoriser une application** et **Bloquer une application**, Comodo Firewall propose – comme ses concurrents – une pratique option **Stopper l'activité réseau** qui permet de bloquer toutes les connexions réseaux entrantes et sortantes sur sa machine.

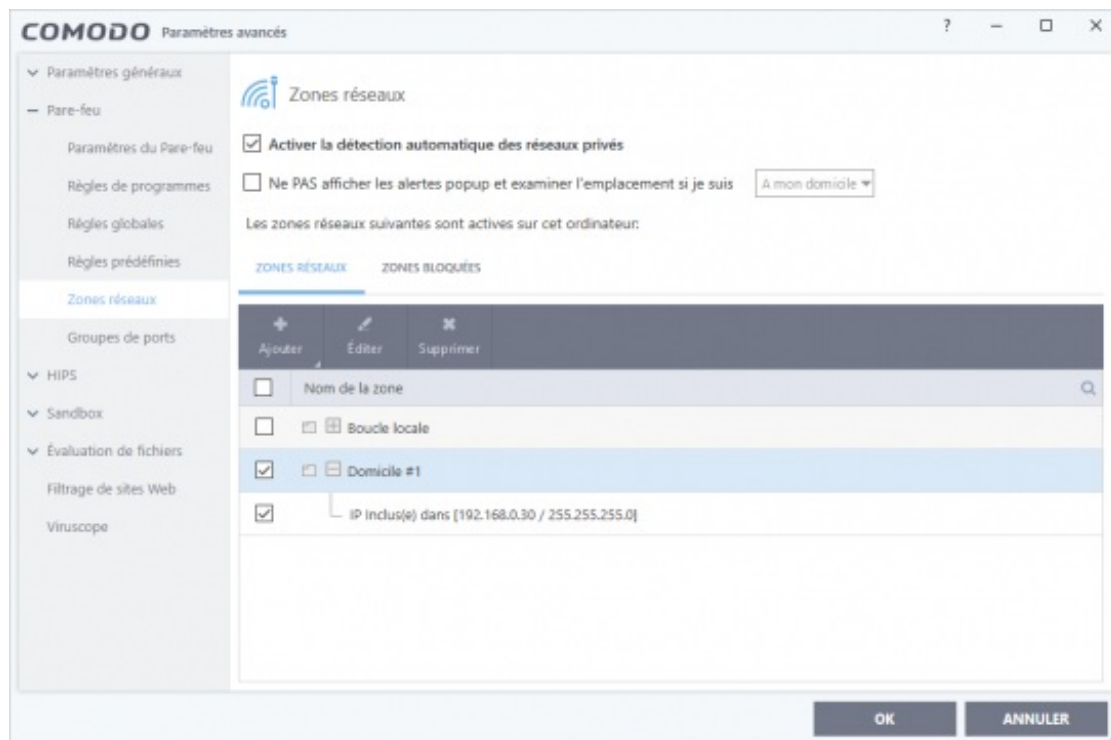


Intéressons-nous maintenant à l'option **Gérer le réseau**. Après l'installation de Comodo Firewall et le redémarrage du PC, Comodo détecte votre connexion réseau et vous demande de **définir la zone réseau** dans laquelle celle-ci se trouve : domicile, travail ou lieu public.



Dans la capture ci-dessus, si vous sélectionnez *MON DOMICILE* par exemple, une zone réseau « Domicile #1 » sera créée pour la connexion au réseau sans-fil sur lequel vous êtes

connecté avec l'adresse IP 192.168.0.30.



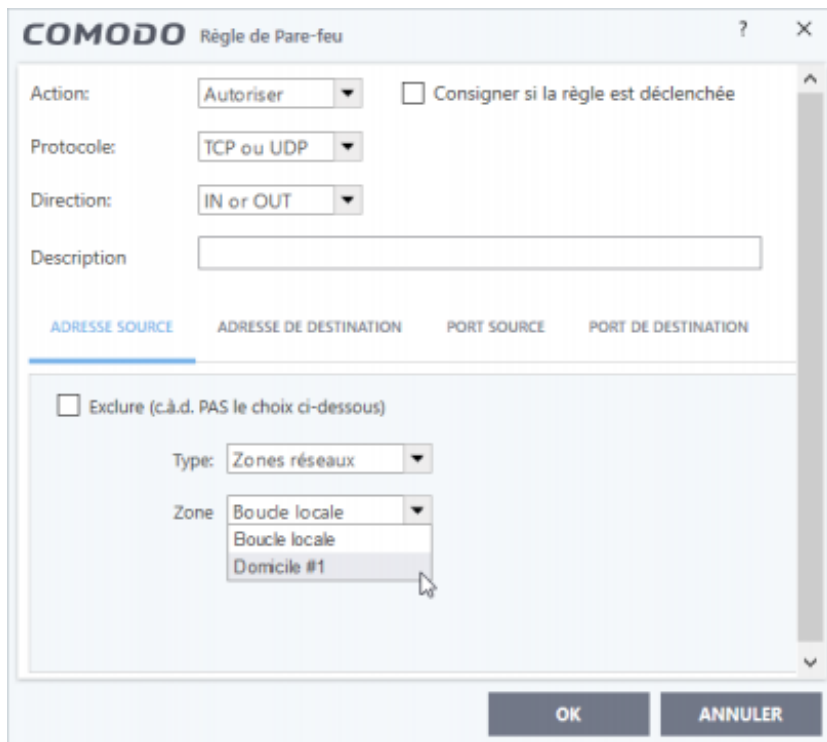
Si votre PC se connecte à un réseau avec l'adresse IP 192.168.0.30, la zone « Domicile #1 » sera appliquée.

Les **zones réseaux dans Comodo Firewall** ne fonctionnent pas de la même façon que dans **ZoneAlarm**. Souvenez-vous : dans ZoneAlarm, un **niveau de sécurité** (élevé ou moyen) est appliqué à une des deux zones existantes (publique ou sûre), zone qu'il est obligatoire de définir pour chacune de ses connexions réseaux. Dans Comodo, **ajouter une zone à un réseau** n'est pas obligatoire et ne définit aucun niveau d'autorisation ou droit d'accès sur ce réseau. Vous pouvez d'ailleurs créer autant de zones réseaux que vous voulez et les attribuer à plusieurs connexions réseaux.

Mais alors à quoi servent ces zones réseaux dans Comodo ?

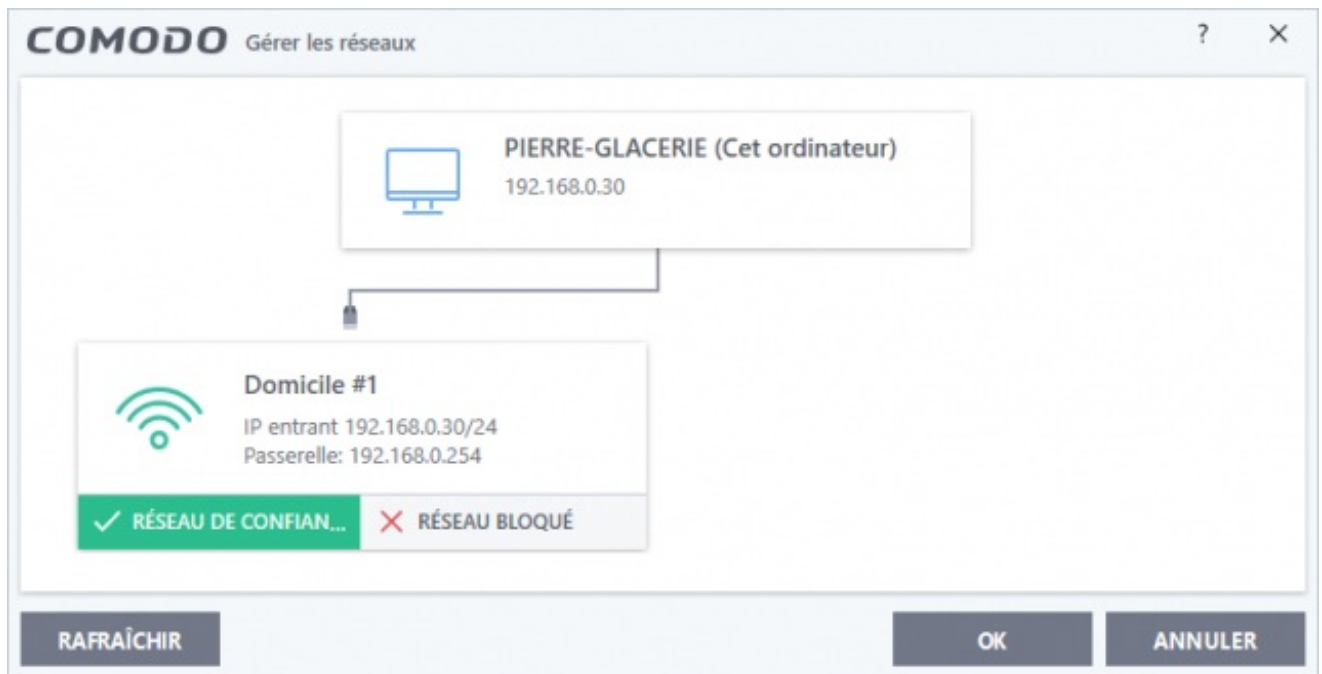
Eh bien dans Comodo, une zone réseau a davantage un aspect pratique :

- Lors de la **création d'une règle de programme**, vous pouvez faire en sorte que cette règle ne s'applique que si votre connexion réseau actuelle se trouve dans la zone « Domicile #1 » par exemple. On peut voir une zone réseau comme un **raccourci** vers une adresse IP, raccourci que l'on peut utiliser lors de la création d'une règle de pare-feu.



Une règle de programme appliquée uniquement à la zone réseau
« Domicile #1 ».

- Une zone réseau peut être définie comme **Réseau de confiance** ou **Réseau bloqué**. Toutes les connexions entrantes et sortantes sont bloquées si une zone réseau est définie en tant que **Réseau bloqué**.



La zone « Domicile #1 » est définie en tant que « Réseau de confiance ». Les connexions réseaux entrantes et sortantes sont autorisées sur cette zone.

Même si ces zones réseaux **ne sont pas d'une importance capitale**, je tenais quand même à vous expliquer leur fonctionnement pour que vous ne fassiez pas le parallèle avec celles sous ZoneAlarm.

Autre option plus intéressante, la possibilité de **cacher les ports** et ce, de deux manières différentes. Pour rappel, que ce soit sur votre réseau local ou sur Internet, votre ordinateur communique (envoie et reçoit des données) avec d'autres ordinateurs au travers de **ports**. Cette option de sécurité permet de **cacher tous ces ports de communication**, rendant votre ordinateur invisible sur le réseau et permettant à celui-ci de ne pas répondre aux scans de ports opportunistes.

Qu'est-ce qu'un **scan de port** ? En quoi est-ce dangereux ?

Une **attaque par « scan de ports »** consiste à envoyer un message à chacun des ports de votre ordinateur. Cette technique est utilisée par les pirates pour savoir quels ports sont ouverts et quels ports sont utilisés par les services sur votre machine. En obtenant cette information, un pirate peut déterminer **quelles attaques sont susceptibles de fonctionner** sur votre machine.

Cacher un port permet de rendre votre **ordinateur invisible à un scan de ports**. A noter, cacher un port n'est pas la même chose que de fermer un port. En cachant un port, **aucune réponse n'est donnée** lors d'une tentative de connexion. En fermant un port, une réponse « fermé » est renvoyée, révélant au pirate qu'il existe réellement un PC. Si un pirate informatique ne peut pas voir les ports de votre ordinateur, il jugera que celui-ci est hors ligne et passera à d'autres cibles. Même avec les ports cachés, vous pouvez **toujours vous connecter à Internet** et transférer des données comme d'habitude, mais vous restez invisibles aux menaces extérieures.



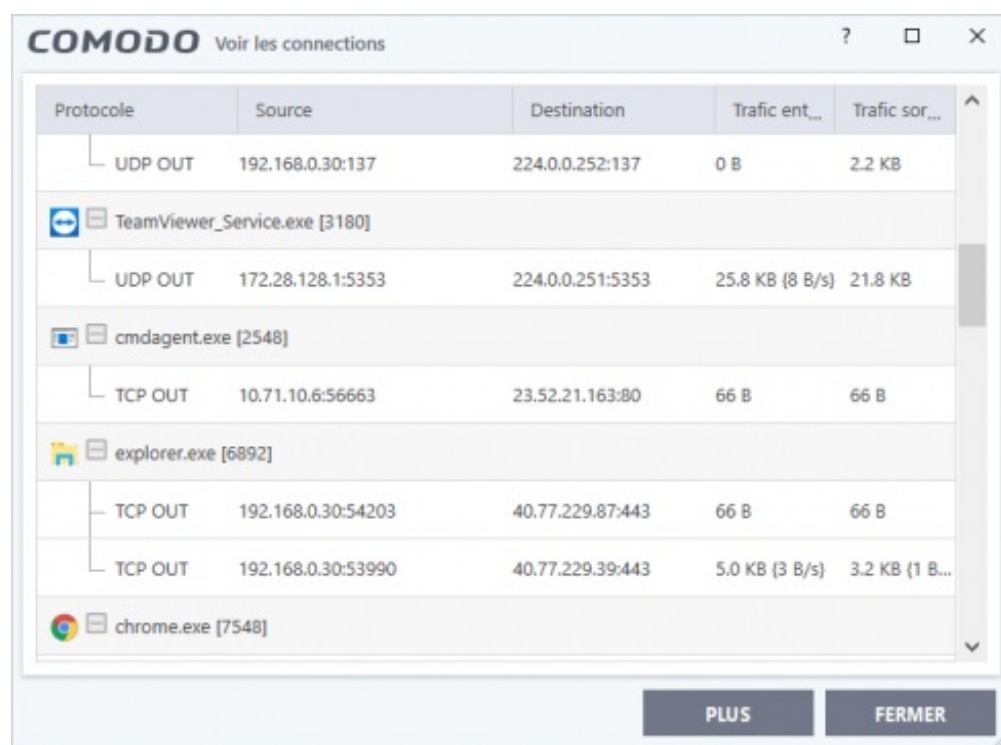
Comodo Firewall vous propose deux options pour **cacher les ports de votre PC** :

- **Bloquer les connexions entrantes** : les ports de votre ordinateur sont invisibles sur tous les réseaux, que vous leur fassiez confiance ou non (cf. **Gérer les réseaux** dans le paragraphe précédent). Si vous êtes à votre domicile et si vous n'utilisez qu'un seul

ordinateur qui ne fait pas partie d'un réseau local, vous avez tout intérêt à utiliser cette option, **la plus pratique et la plus sécurisée**. Vous n'êtes pas averti lorsqu'une connexion entrante est bloquée, mais une entrée est ajoutée dans le fichier journal des événements du pare-feu.

- **Alertes sur les connexions entrantes** : un avertissement de pare-feu s'affiche chaque fois qu'il y a une demande pour une connexion entrante. L'alerte vous demande si vous voulez ou non que la connexion se fasse. Cette option peut être utile pour des applications telles que des programmes P2P et les applications de bureau à distance qui nécessitent une visibilité de certains ports pour se connecter à votre machine.

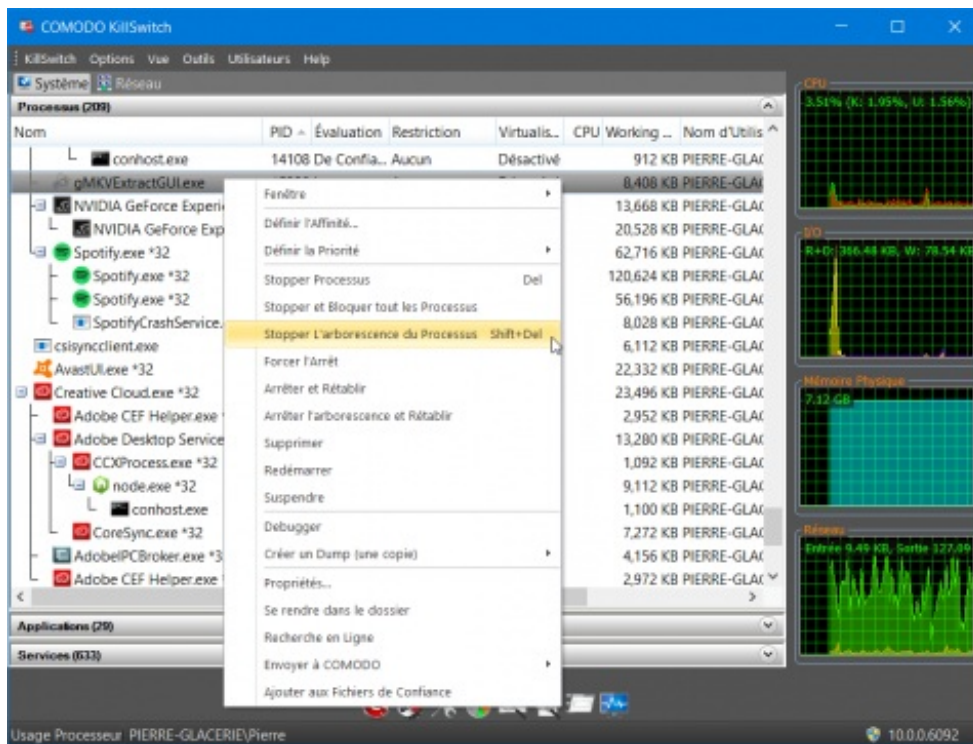
Comodo propose également une option permettant de voir les **applications qui sont connectées à Internet**. Bien que complet, on est ici très loin de la clarté de [GlassWire](#) qui propose un graphique simple et facile d'accès pour visualiser rapidement les connexions entrantes et sortantes de chaque application.



The screenshot shows the 'COMODO Voir les connexions' window. It displays a table of active network connections with columns for Protocol, Source, Destination, Incoming Traffic, and Outgoing Traffic. Applications like TeamViewer, cmdagent.exe, explorer.exe, and chrome.exe are listed on the left, each with its PID. Buttons for 'PLUS' and 'FERMER' are at the bottom right.

Protocole	Source	Destination	Trafic ent...	Trafic sor...
UDP OUT	192.168.0.30:137	224.0.0.252:137	0 B	2.2 KB
TeamViewer_Service.exe [3180]				
UDP OUT	172.28.128.1:5353	224.0.0.251:5353	25.8 KB (8 B/s)	21.8 KB
cmdagent.exe [2548]				
TCP OUT	10.71.10.6:56663	23.52.21.163:80	66 B	66 B
explorer.exe [6892]				
TCP OUT	192.168.0.30:54203	40.77.229.87:443	66 B	66 B
TCP OUT	192.168.0.30:53990	40.77.229.39:443	5.0 KB (3 B/s)	3.2 KB (1 B/s)
chrome.exe [7548]				

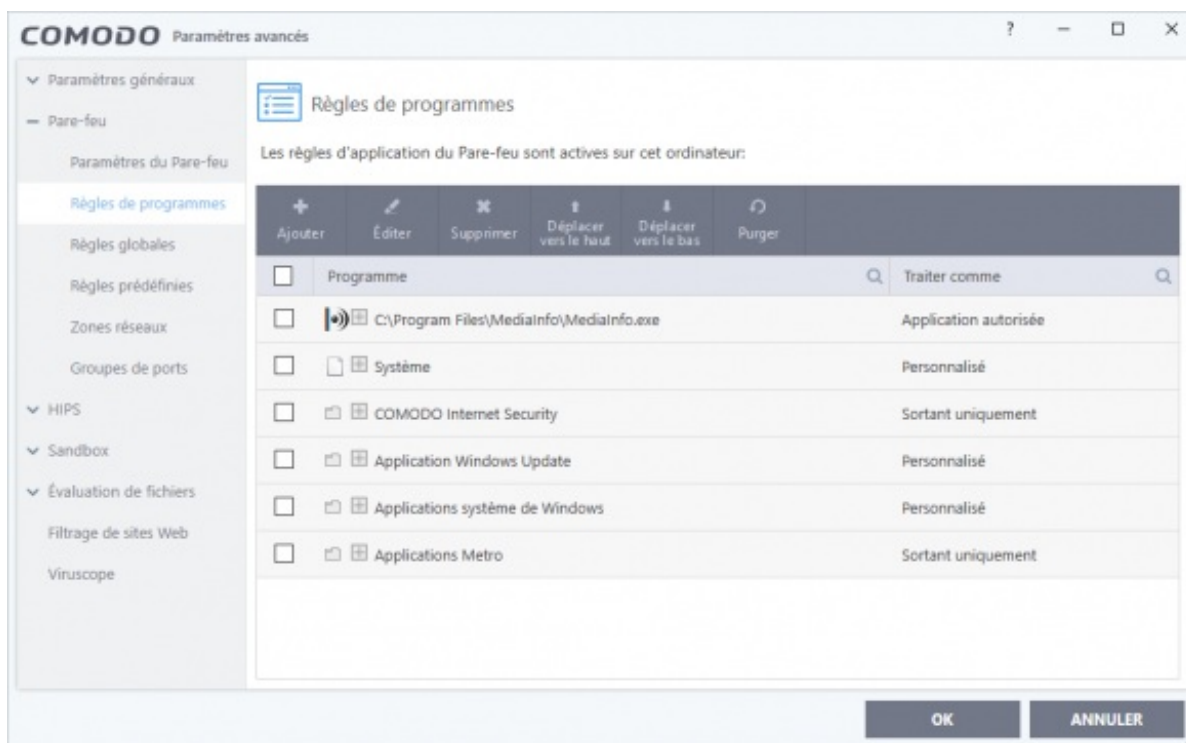
Néanmoins, via le bouton **Plus**, Comodo peut installer et lancer **Comodo KillSwitch**, un outil de surveillance du système qui permet d'identifier, de surveiller et de terminer tous les processus dangereux qui s'exécutent sur le système. KillSwitch est vraiment très complet et réservé aux utilisateurs avancés. Toutefois, la lecture de l'activité réseau reste toujours moins facile que sur GlassWire.



Comodo KillSwitch

Comme tout bon firewall qui se respecte, Comodo Firewall dispose d'un **système de règles** pour autoriser ou refuser l'accès Internet ou réseau à une application. Il n'est pas inutile de le préciser car les versions payantes de GlassWire ne disposent pas d'une telle fonctionnalité et cette dernière n'est disponible que dans la version PRO de ZoneAlarm.

Petit rappel sur le **système de règles dans les pare-feux** : chaque fois qu'une application fait une demande d'accès Internet ou réseau, **Comodo Firewall** (et tous les pare-feux basés sur un système de règles) autorise ou refuse cette demande en fonction des règles de pare-feu définies pour cette application : autoriser ou bloquer la connexion, sur quel type de connexion (entrante ou sortante), sur quels protocoles (TCP ou UDP), sur quels ports...

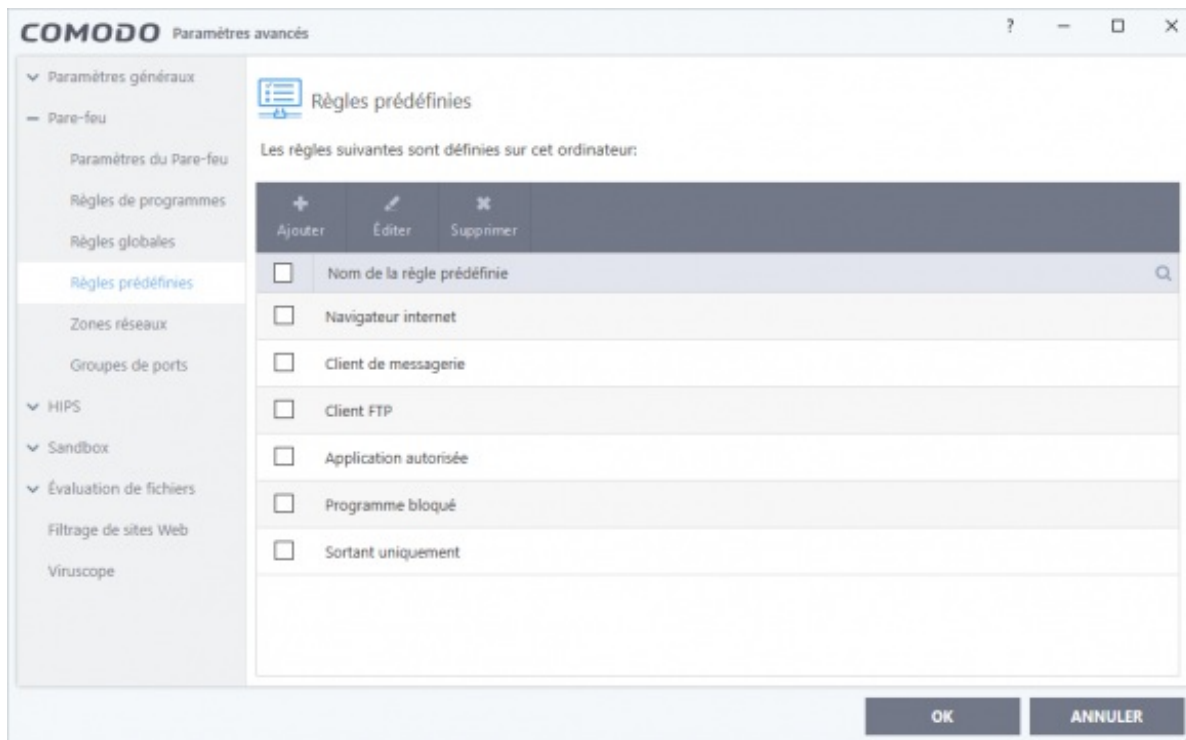


Toutes les règles de programmes définies dans le pare-feu de Comodo

Si vous avez choisi le **mode sécurisé (mode par défaut)**, Comodo créera tout seul les autorisations d'accès pour les applications qu'il considère comme saines. Vous ne serez pas sollicité et ne recevrez pas d'alertes quand ces applications se connecteront à Internet. C'est assez déroutant au départ, on a l'impression que le pare-feu ne fonctionne pas ! Si vous souhaitez avoir plus de contrôle et de visibilité sur l'activité réseau de votre machine, passez en **mode personnalisé**.

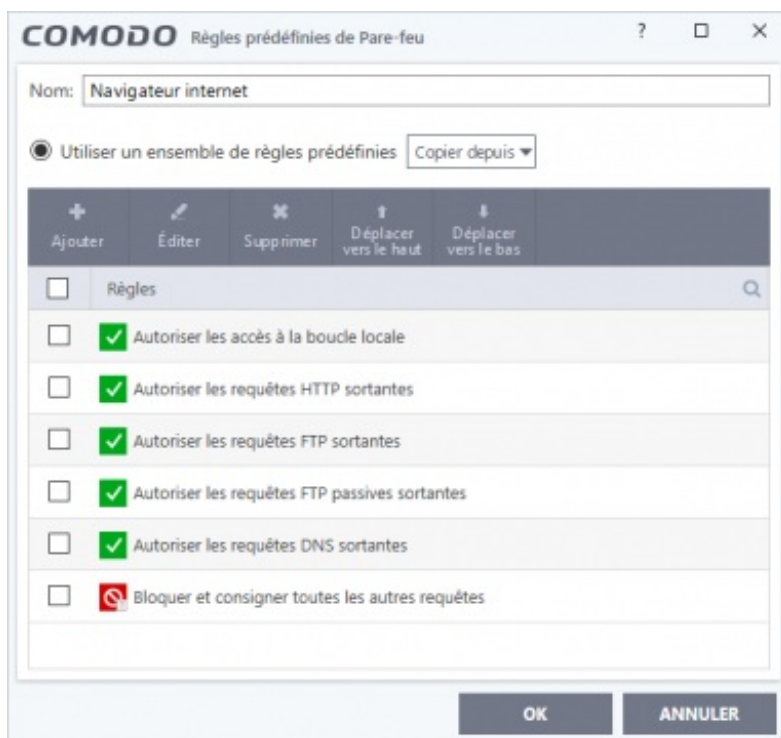
Petite particularité : les **règles « Autoriser » pour les applications considérées comme saines ne sont pas automatiquement créées** par Comodo dans le but de rendre la fenêtre des règles plus claire et de réduire les ressources système. Dans la fenêtre des règles de programmes ci-dessus par exemple, on ne voit qu'une seule règle personnalisée pour un programme non considéré comme sain par Comodo (MediaInfo). Les règles pour tous mes autres programmes (Mozilla Firefox, Spotify, NotePad++...), bien qu'existantes, ne sont pas affichées. Il est néanmoins toujours possible de réactiver ce paramètre en activant l'option *Créer des règles pour des applications saines*.

Pratique, Comodo Firewall dispose d'un **système de règles prédéfinies** : navigateur Internet, client de messagerie, client FTP, application autorisée, programme bloqué et sortant uniquement.



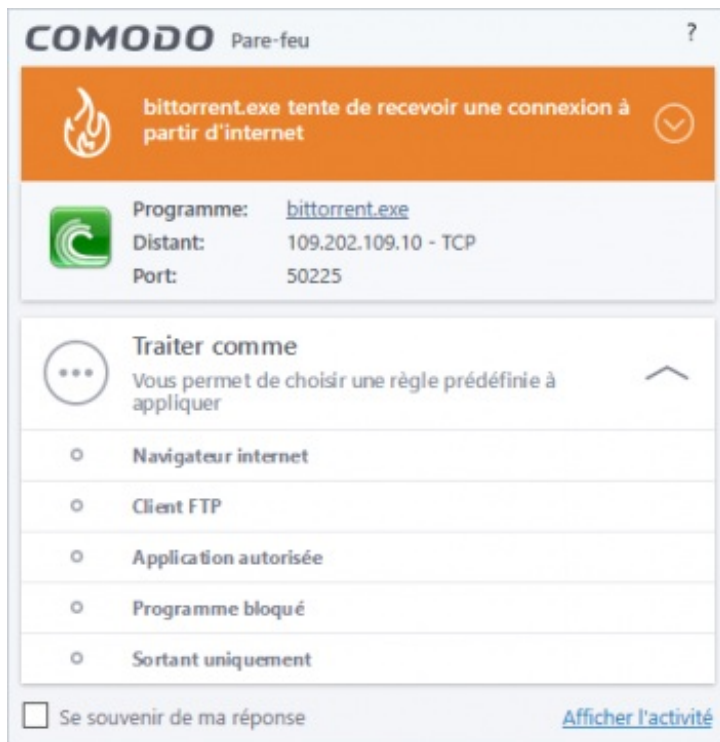
Les règles prédéfinies du pare-feu de Comodo.

Une règle prédéfinie contient un **ensemble de règles spécifiques à un usage**. Par exemple la règle prédéfinie « Navigateur Internet » contient des règles qui autorisent les requêtes HTTPS, FTP et DNS sortantes et bloquent toutes les autres requêtes.



Les règles de la règle prédéfinie « Navigateur Internet ».

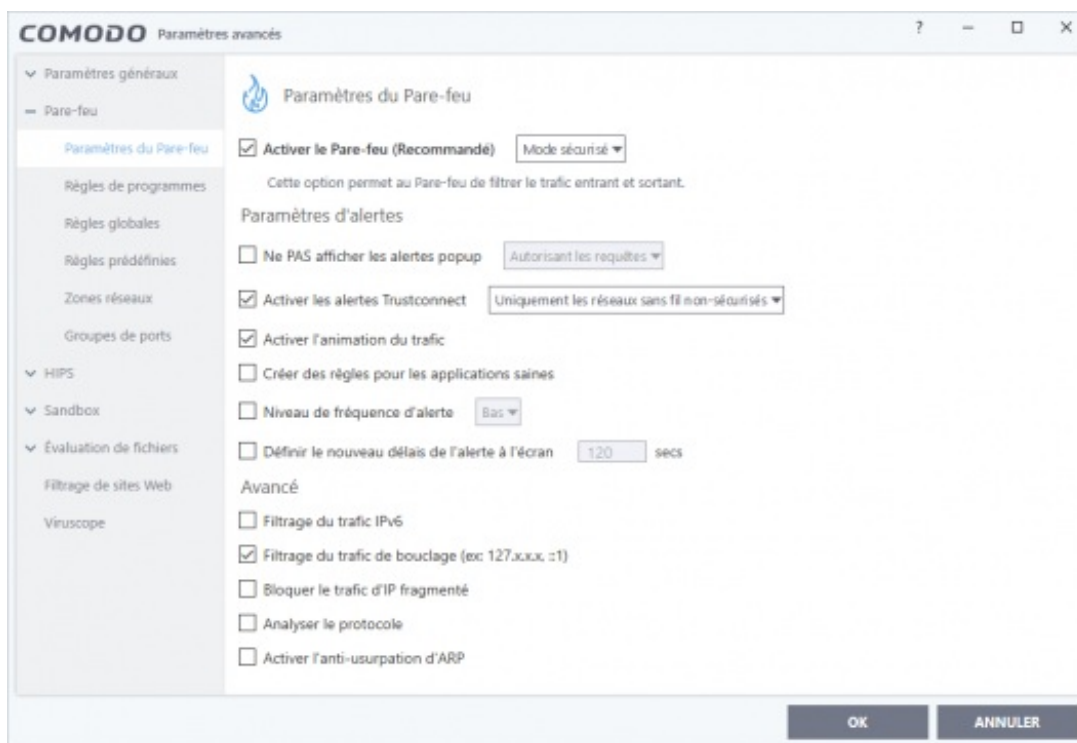
Vous pouvez créer autant de règles que vous le voulez. On retrouve ces règles prédéfinies lors d'une alerte de pare-feu : en plus des classiques **Autoriser** et **Bloquer**, on peut appliquer une **règle prédéfinie** à l'application qui demande une connexion à Internet.



Choix d'une règle prédéfinie pour le programme BitTorrent qui demande à recevoir une connexion à partir d'Internet (mode personnalisé).

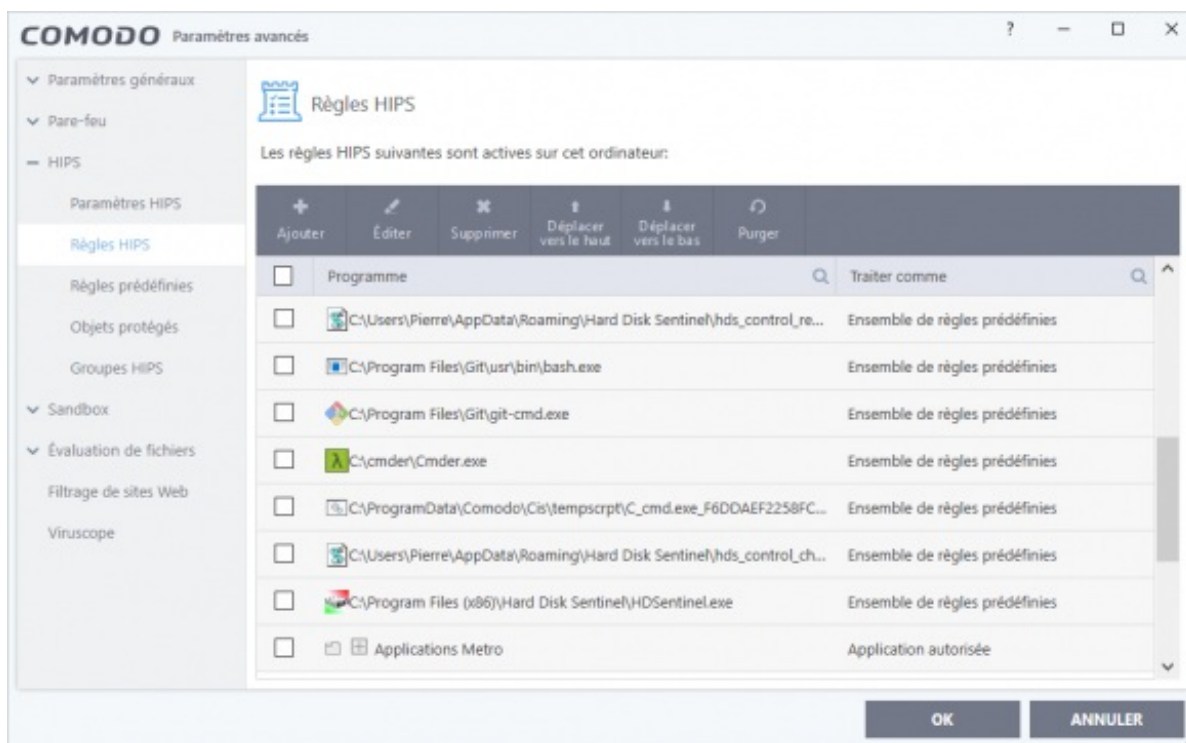
Les utilisateurs novices comme expérimentés trouveront leur bonheur avec les **règles de programmes de Comodo Firewall**. On peut **créer des règles très précises** pour autoriser/bloquer l'accès à Internet ou au réseau à une application, le tout dans une interface claire et simple d'utilisation.

Enfin, Comodo Firewall dispose comme ZoneAlarm PRO d'**options de sécurité avancées**. Pour plus d'informations sur ces options avancées du pare-feu (filtrage du trafic IPv6, bloquer le trafic d'IP fragmenté, anti-ursupation d'ARP...), vous pouvez consulter l'aide : <https://help.comodo.com/topic-72-1-766-9172-General-Firewall-Settings.html> (en anglais).



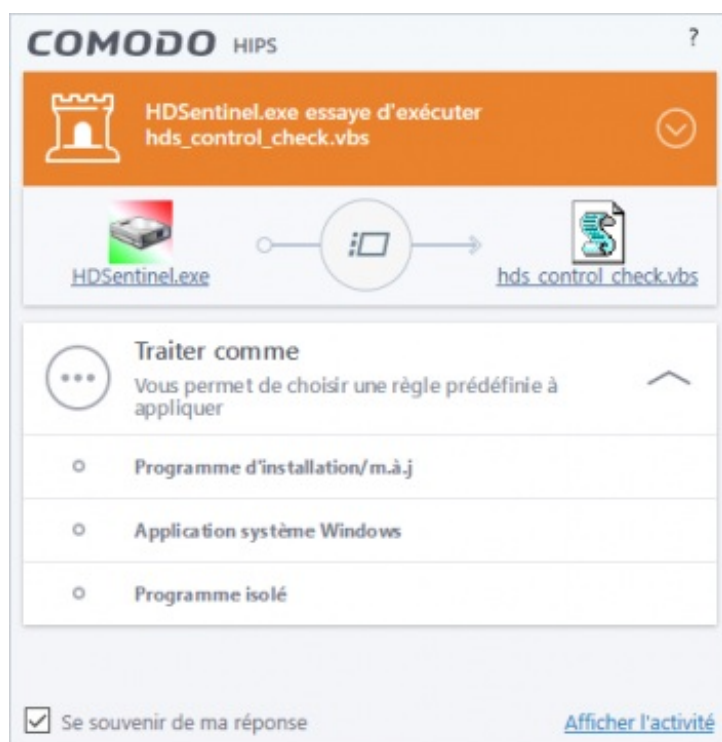
HIPS

Comodo Firewall n'est pas qu'un simple pare-feu, il dispose également d'un **système de prévention d'intrusion** appelé **HIPS** (Host Intrusion Protection System). Le système Host Intrusion Protection est un composant qui **surveille constamment l'activité du système** et qui permet seulement aux exécutables et aux processus qui respectent les règles de sécurité définies l'utilisateur de s'exécuter. Par défaut, Comodo Firewall s'installe avec un **jeu de règles HIPS déjà en place**. Par exemple, HIPS protège automatiquement les fichiers et dossiers sensibles du système et les clés de registre afin d'empêcher toute modification non autorisée par des programmes malveillants.



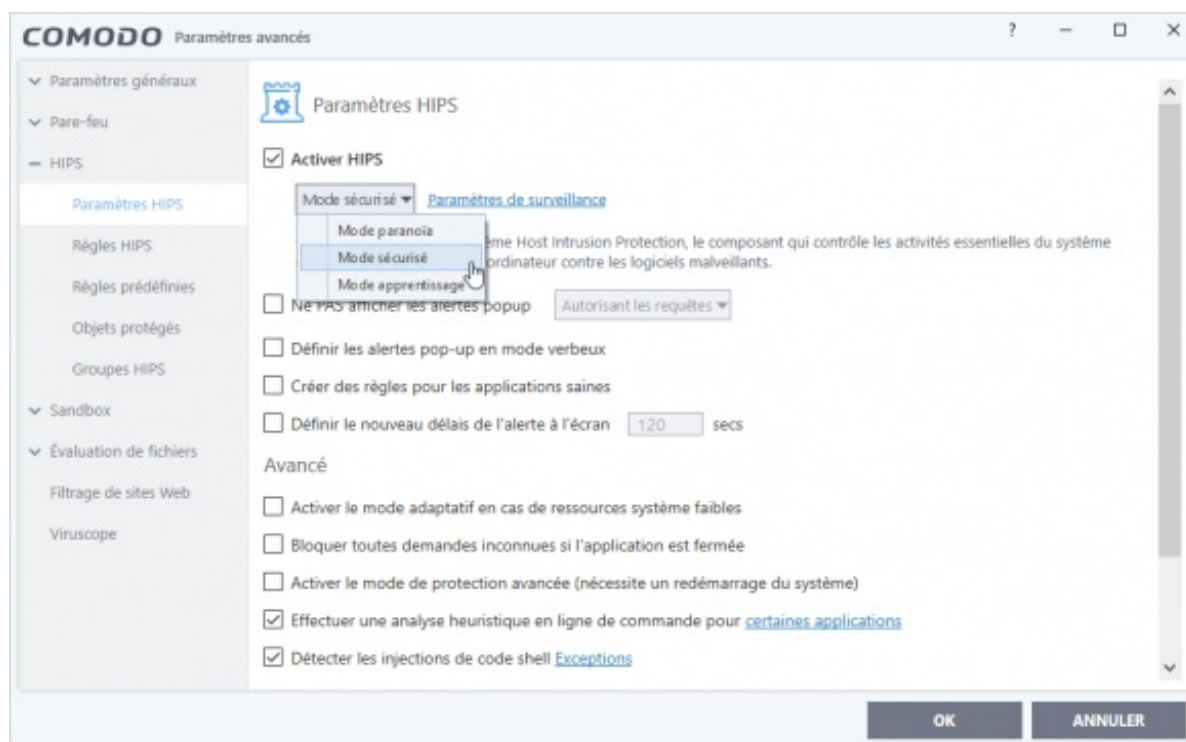
HIPS est disponible en deux modes de fonctionnement :

- **Mode personnalisé** : le niveau de sécurité le plus élevé. HIPS surveille et contrôle tous les fichiers exécutables en dehors de ceux que vous avez jugé sûrs. Comodo Firewall n'essaie pas d'apprendre le comportement de chaque application et **n'utilise que vos paramètres de configuration** pour filtrer l'activité du système. De même, Comodo Firewall ne crée pas automatiquement de règles « Autoriser » pour les exécutables, c'est **vous et vous seul** qui devez autoriser ou bloquer l'activité d'un programme. Le mode personnalisé **génère énormément d'alertes HIPS** et est recommandé pour les utilisateurs avancés qui veulent une **connaissance complète de l'activité du système**.
- **Mode sécurisé** : tout en surveillant l'activité du système, HIPS **apprend automatiquement l'activité des exécutables et des applications** certifiées « saines » par Comodo : il crée automatiquement des règles « Autoriser » pour ces activités (si l'option *Créer des règles pour des applications saines* est cochée). Pour les applications non certifiées ou inconnues, vous **recevrez une alerte** chaque fois qu'une application tentera de s'exécuter. Vous pouvez par exemple ajouter une nouvelle application à la liste blanche de Comodo en choisissant *Traiter comme une application approuvée* sur l'alerte Comodo. Cela indique à HIPS de ne pas générer d'alerte la prochaine fois que l'application s'exécute. Le mode sécurisé est **recommandé pour la plupart des utilisateurs**.

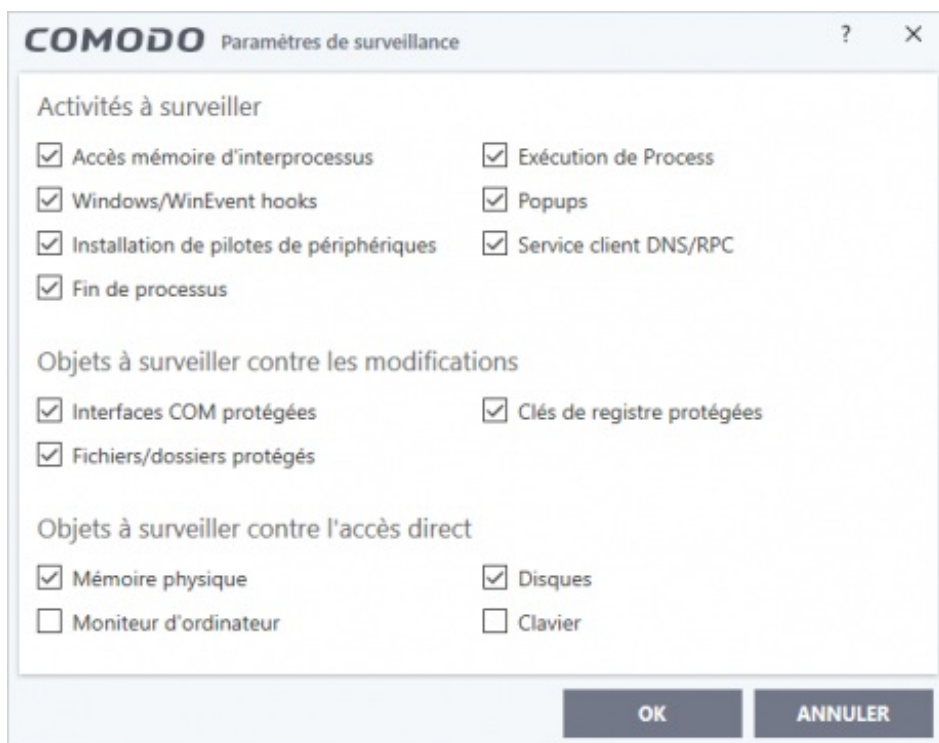


Alerte HIPS : l'application HDSentinel tente d'accès au fichier hds_control_check.vbs.

- **Mode apprentissage** : HIPS surveille et apprend l'activité de tous les exécutable et crée automatiquement des règles « Autoriser » pour chaque programme. Vous ne recevez aucune alerte HIPS en mode apprentissage. **Toutes les applications sont autorisées à s'exécuter.** A utiliser en cas de nécessité absolue !



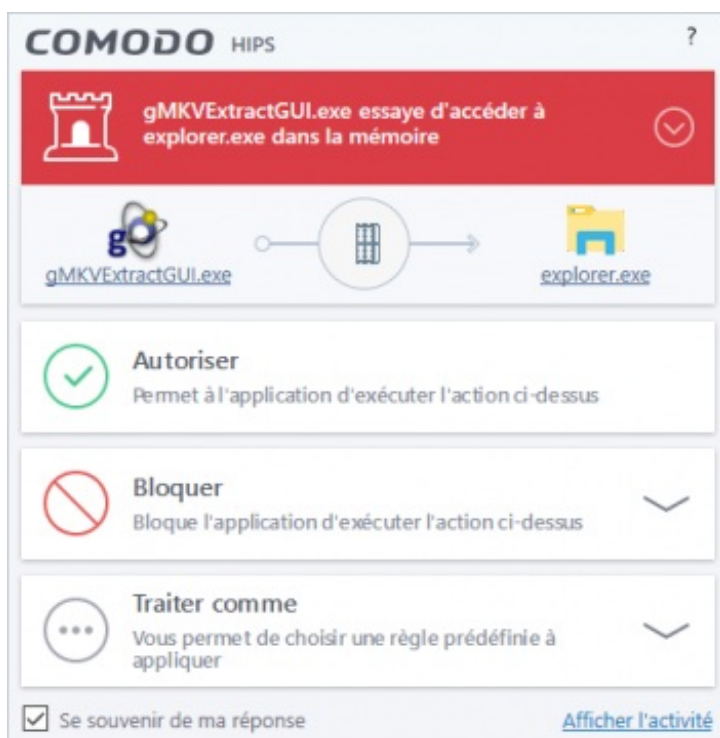
Vous pouvez choisir les **activités et les objets à surveiller** dans les paramètres de surveillance :



Le module HIPS fonctionne un peu de la **même manière que le module pare-feu**: on a des règles personnalisées, des règles prédéfinies...

D'accord, comment ça se passe dans la vraie vie ?

Quand une **application non certifiée par Comodo ou inconnue** tente d'accéder à une autre ressource du système, une alerte HIPS s'affiche. Dans la capture ci-dessous, l'application gMKVExtractGUI tente d'exécuter l'explorateur Windows dans le but de sélectionner des fichiers MKV à traiter.

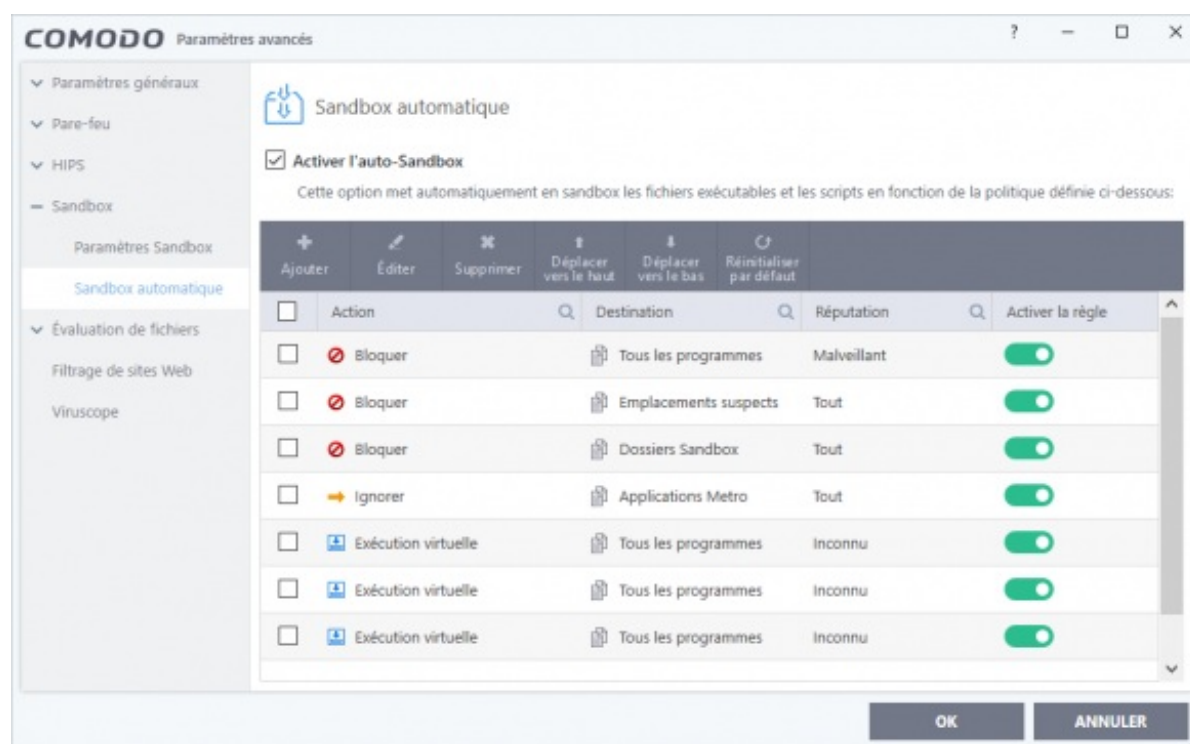


Tout comme le module pare-feu, vous avez le choix entre **Autoriser**, **Bloquer** et **Traiter comme** (choix d'une règle prédéfinie). C'est aussi simple que ça ! En fonctionnant de la sorte, HIPS vous permet d'identifier et de bloquer les actions suspectes.

Pour plus d'informations sur l'ensemble des paramètres disponibles pour l'HIPS de Comodo : <https://help.comodo.com/topic-72-1-766-9163-HIPS-Settings.html> (en anglais).

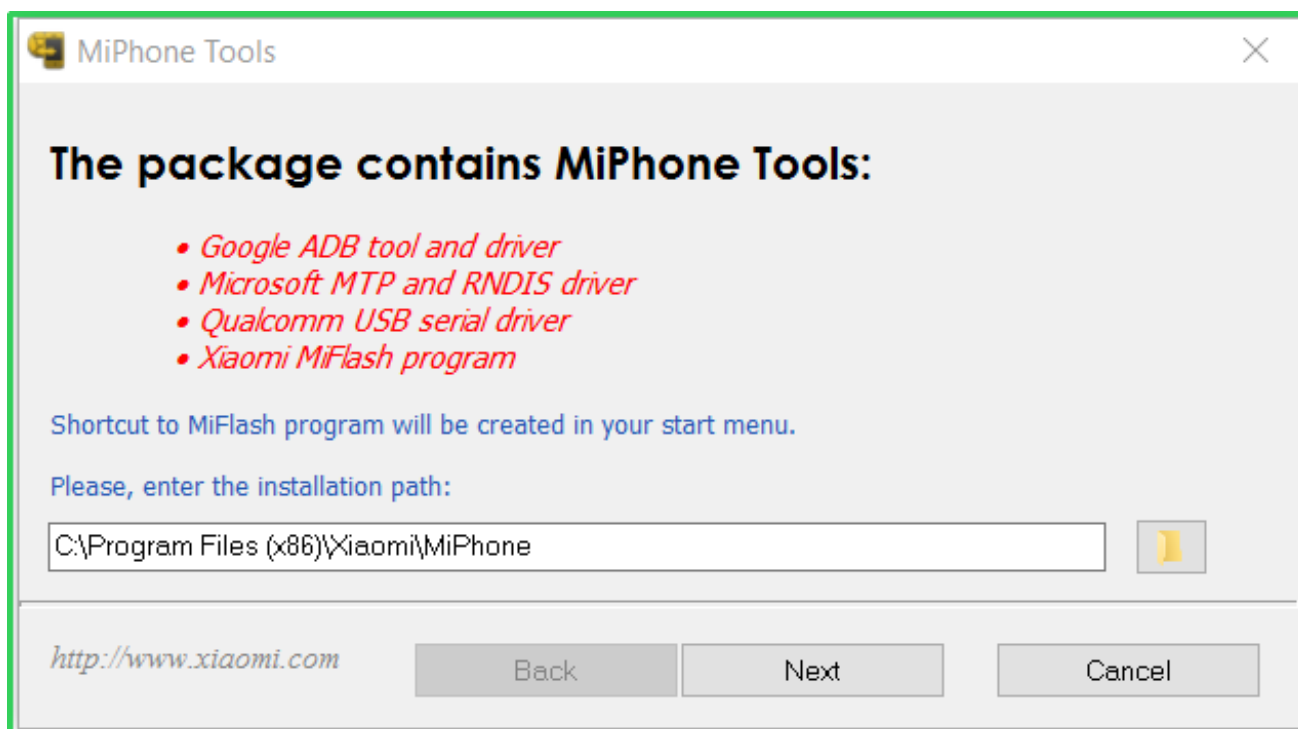
Auto-sandbox

La sandbox ou « bac à sable » un environnement virtuel destinés aux applications inconnues et non fiables. Si **Comodo Firewall** détecte un fichier dont le statut de confiance est « Inconnu », il exécutera automatiquement ce fichier dans cette **sandbox**. Les fichiers qui s'exécutent dans la sandbox sont **isolés du reste de l'ordinateur** pour les empêcher de causer des dommages sur votre système et vos données.



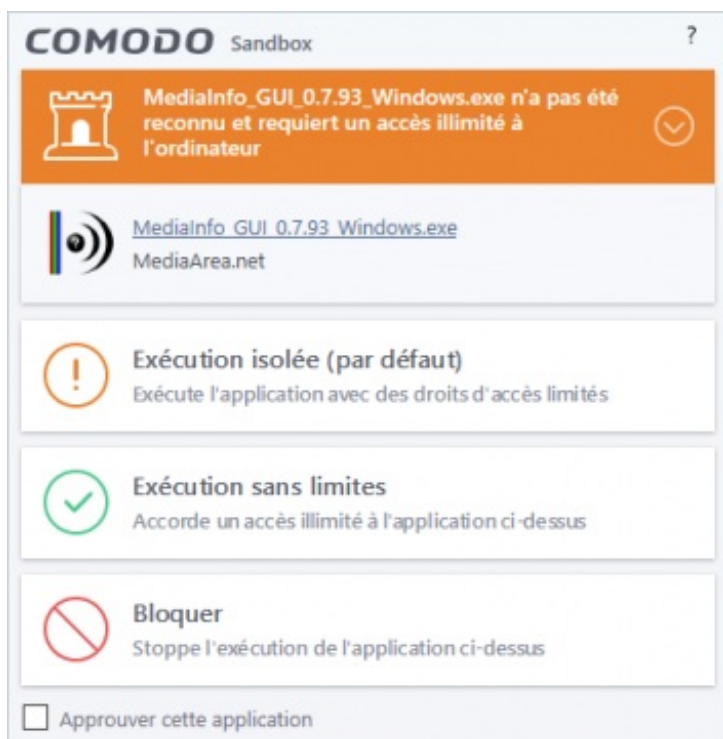
Pratique, la sandbox de Comodo dispose d'un **espace partagé** dans

C:\ProgramData\Shared Space pour partager les fichiers entre les applications qui s'exécutent dans le bac à sable et le « vrai » système de fichiers. Les applications « sandboxées » peuvent stocker des données dans cet espace partagé pour les futures sessions, données qui sont aussi accessibles par les applications réelles de votre système.



L'application MiPhone Tools, non reconnu par Comodo, est exécutée dans la sandbox. La fenêtre de l'application est mise en surbrillance pour distinguer les applications sandboxées.

Si un programme inconnu par Comodo requiert les **droits administrateurs** ou des privilèges élevés pour s'exécuter, Comodo Firewall affichera une alerte. Un programme d'installation autorisé à s'exécuter avec des privilèges élevés peut apporter des modifications à des zones importantes de l'ordinateur telles que le Registre, il convient donc d'être prudent.

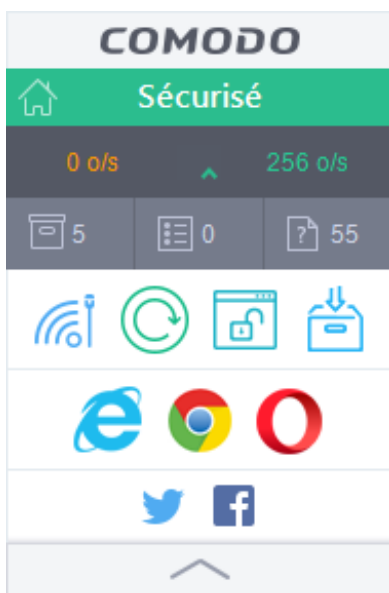


Alerte sandbox après l'exécution du programme d'installation de MediaInfo, application inconnue à Comodo.

Plusieurs choix s'offrent à vous :

- Si vous faites **confiance à l'éditeur du logiciel**, vous pouvez cliquer « Exécution sans limites ». Cela accordera les droits administrateur à l'application et permettra au programme d'installation de s'exécuter.
- Si vous **n'êtes pas sûr du logiciel**, exécutez-le avec un accès restreint en cliquant sur « Exécution isolée ».
- Si cette **alerte est inattendue**, vous devriez interrompre l'application en cliquant sur le bouton « Bloquer ».
- Si vous sélectionnez « Approuver cette application », Comodo Firewall inclura le fichier dans la **liste des fichiers approuvés de Comodo** et aucune alerte ne sera générée ultérieurement lorsque vous exécuterez la même application.

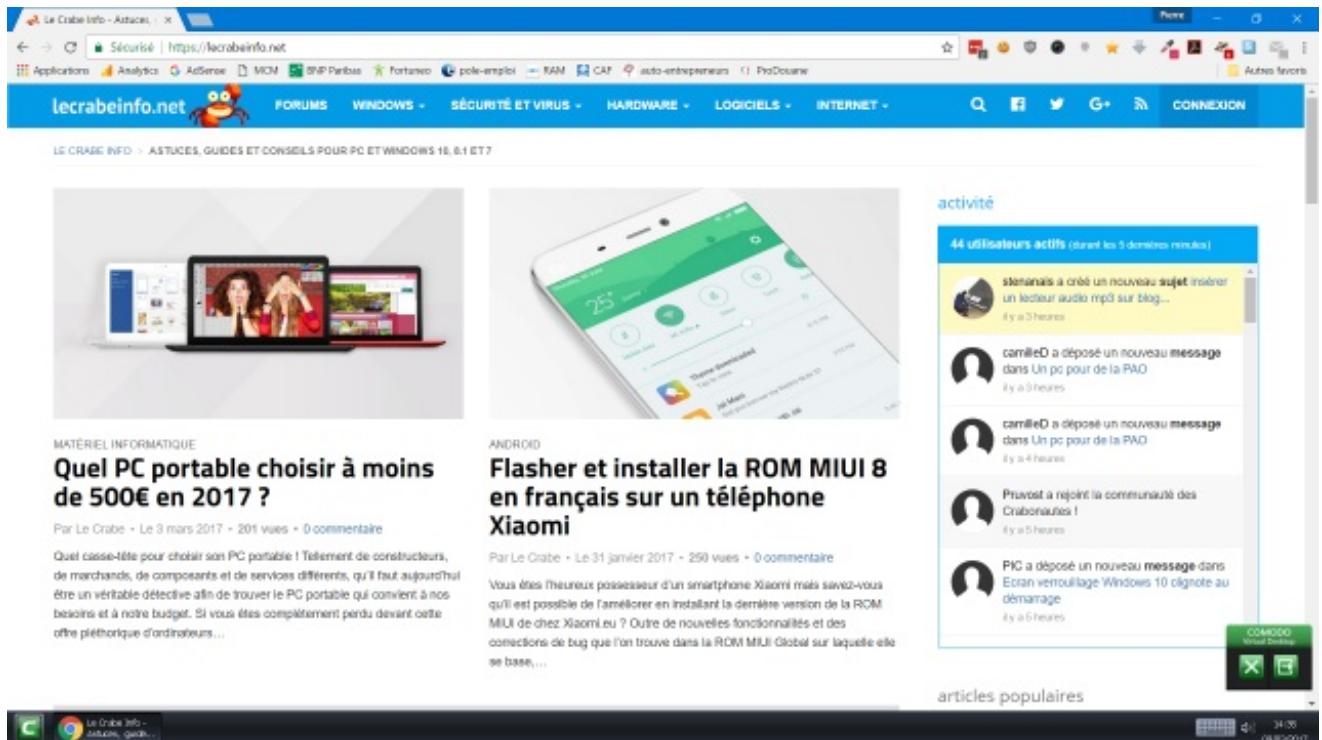
Dernière petite chose concernant la **sandbox** : Comodo affiche par défaut un widget sur le bureau Windows. Bien que je ne sois pas fan de ce genre d'outil, il s'avère que celui de Comodo est plutôt pratique. Il permet de **voir l'activité réseau en cours** et d'accéder à des **raccourcis utiles** comme voir les applications qui fonctionnent actuellement dans la sandbox, les fichiers non reconnus en attente d'analyse, les applications bloquées... Mais il permet aussi de **lancer les navigateurs Web de votre PC directement dans la sandbox**! Quand on sait que les menaces peuvent aussi venir du navigateur Web, il n'est pas inutile de lancer son Chrome, Firefox ou Opera dans la sandbox pour protéger son système des logiciels malveillants.



A la fois simple d'utilisation et puissant, le système de sandbox de Comodo **augmente drastiquement la sécurité de l'ordinateur**.

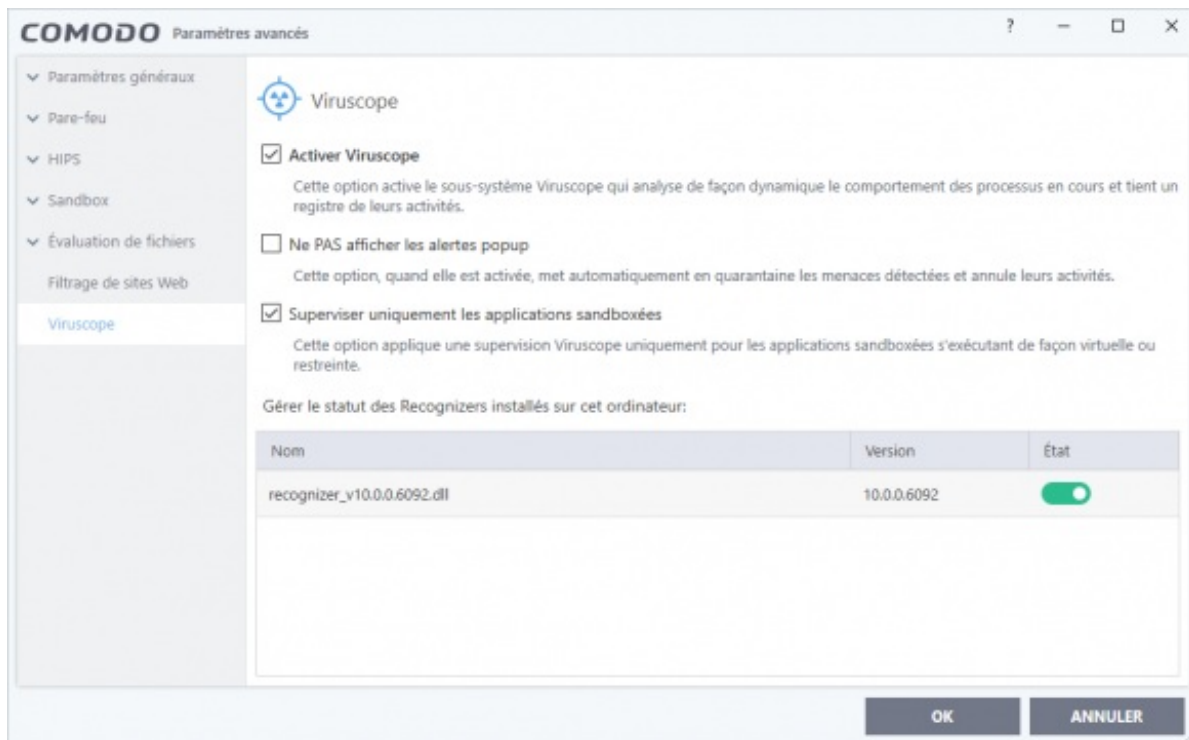
Autres fonctionnalités

- **Bureau virtuel** : un environnement de bureau virtuel dans lequel pour vous pouvez exécuter des programmes et visiter des sites Web dans lesquels vous n'avez pas confiance à 100%. Les applications et les navigateurs Web que vous exécutez à l'intérieur du bureau virtuel ne laissent aucun historique. Tout comme la sandbox, cela vous protège des logiciels malveillants étant donné que toutes les activités qui se déroulent dans le bureau virtuel sont isolées et n'accèdent jamais au système de fichier réel.

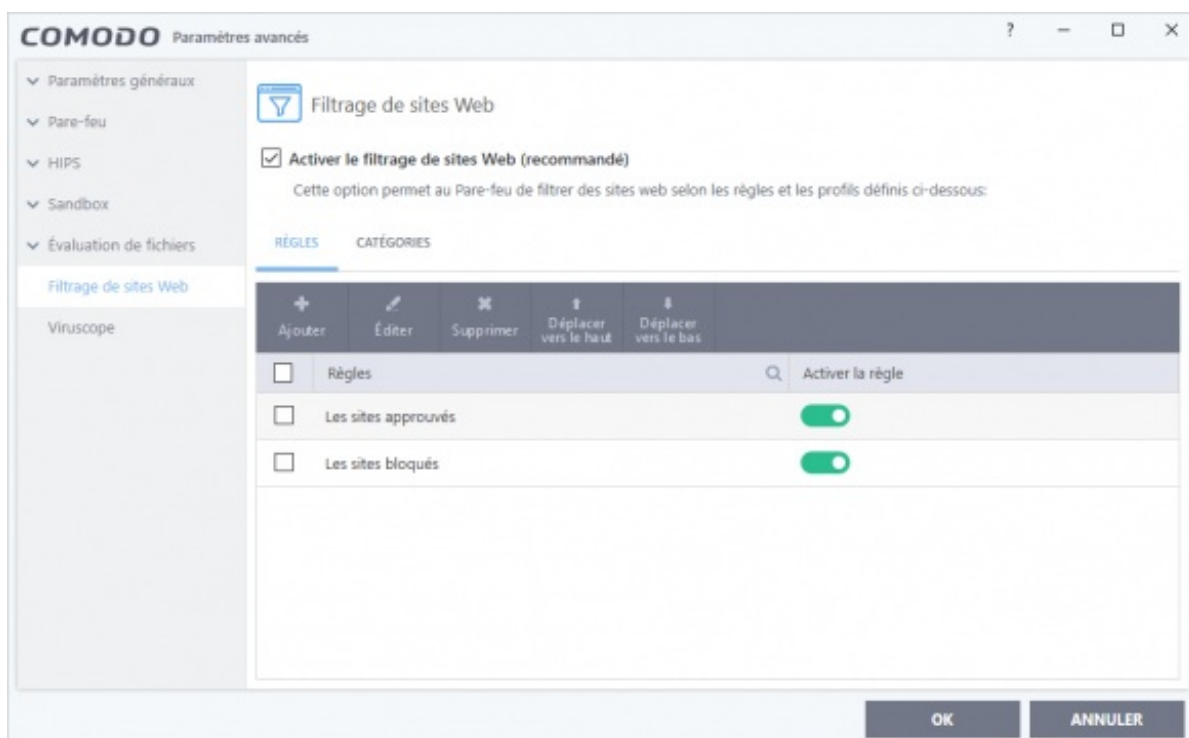


Navigateur Web Google Chrome exécuté dans le bureau virtuel de Comodo. Le bouton en bas à droite permet de switcher entre Windows et le bureau virtuel.

- **Viruscope** : analyse le comportement des processus en cours d'exécution, tient un registre de leurs activités et vous avertit si leurs actions pourraient potentiellement menacer votre vie privée et/ou de sécurité. Je n'ai pas eu l'occasion de tester véritablement cette fonctionnalité.



- **Filtrage de sites Web** : permet d'autoriser ou de bloquer l'accès à des sites Web spécifiques. Des règles peuvent être créées pour des utilisateurs spécifiques de votre ordinateur. Vous avez la possibilité de créer un journal d'événement chaque fois qu'un utilisateur tente de visiter un site Web qui est en conflit avec une règle de filtrage.



Verdict de Comodo Firewall

Comodo Firewall 10

Version testée : Windows, v10.0.0.6092

Système de test : Windows 10 Pro 64 bits

+

Points positifs

- Interface utilisateur claire et intuitive pour une suite de sécurité ultra complète
- Simple d'utilisation pour les débutants, complet pour les utilisateurs avancés
- Comodo Safe List : liste blanche d'éditeurs, de programmes et de fichiers certifiés
- Pare-feu simple et complet avec système de règles de programmes
- Host Intrusion Protection System (HIPS)
- Sandbox et bureau virtuel
- Gratuit

–

Points négatifs

- Configuration Yahoo! proposée à deux reprises lors de l'installation
- Visualisation de l'activité réseau pas pratique, bien que complète

Que dire de Comodo Firewall ? Simple, ultra complet et 100% gratuit, c'est sans aucun doute la suite de sécurité la plus complète que l'on peut trouver à l'heure actuelle. L'utilisateur a vraiment le sentiment d'être protégé grâce à tous les outils de sécurité offerts par l'application de Comodo : pare-feu, sandbox, HIPS, bureau virtuel... Comodo frappe un grand coup dans l'univers des logiciels de sécurité avec un logiciel qui serait dommage de réduire à un simple pare-feu. Comodo Firewall est un incontournable, que ce soit pour les débutants ou les utilisateurs expérimentés.



5/5

Table des matières

Dossier : Comparatif de 4 pare-feux : quel firewall/pare-feu choisir pour Windows en 2017 ?

1. Comparatif de 4 pare-feux : quel firewall/pare-feu choisir pour Windows en 2017 ?

2. Test de GlassWire, pare-feu et outil de surveillance de trafic réseau
3. Test de ZoneAlarm Firewall, le pionnier des pare-feux personnels
4. **Test de Comodo Firewall : pare-feu, HIPS, sandbox et plus encore !**

[← Précédent](#)

[#bac à
sable](#)

[#comodo firewall](#)

[#firewall](#)

[#hips](#)

[#pare-feu](#)

[#pare-feu
windows](#)

[#sandbox](#)

[#suite de sécurité](#)

Partagez cet article !



A voir également sur le forum

Test de Comodo Firewall : pare-feu, HIPS, sandbox et plus encore !

[insérer un lecteur audio mp3 sur blog...](#)

[Programme développé en VB 5](#)

[Tester Linux pour le developpement](#)

[Probleme de souris et clavier lors de l insertion du cd image systeme](#)

[Hyper V](#)

Besoin d'aide ?

Malgré la lecture de l'article « **Test de Comodo Firewall : pare-feu, HIPS, sandbox et plus encore !** », vous avez encore des questions qui vous trottent dans la tête ? Vous avez toujours les **mêmes problèmes** qu'au départ ? **Vous êtes bloqués** et vous ne savez plus quoi faire ?

Faites appel à la communauté du Crabe en posant votre question sur le forum !

poser ma question sur le forum

Aucun commentaire

⚠ A LIRE AVANT DE LAISSER UN COMMENTAIRE !

Depuis l'ouverture du [forum d'aide](#), **les commentaires ne sont plus destinés à recevoir des demandes d'aide**. Ils sont désormais là pour recueillir vos remarques sur le contenu de l'article, suggérer des améliorations, donner votre avis sur l'efficacité des solutions proposées...

Bref, vous l'aurez compris, si vous avez besoin d'une assistance : **posez votre question sur le forum d'aide** ! 😊



Nom*

Email*

Participer à la discussion...

- ☐ Parole de crustacé, je jure que mon commentaire n'est pas destiné à demander de l'aide. Je sais qu'il y a le [forum](#) qui est là pour ça. Bon maintenant, laisse-moi commenter !

Submit Comment