Tutoriel COMODO Internet Security
1/ Installation et configuration

Ed 04 : Rédacteur : Michel Dumontet d : 17/09/2020

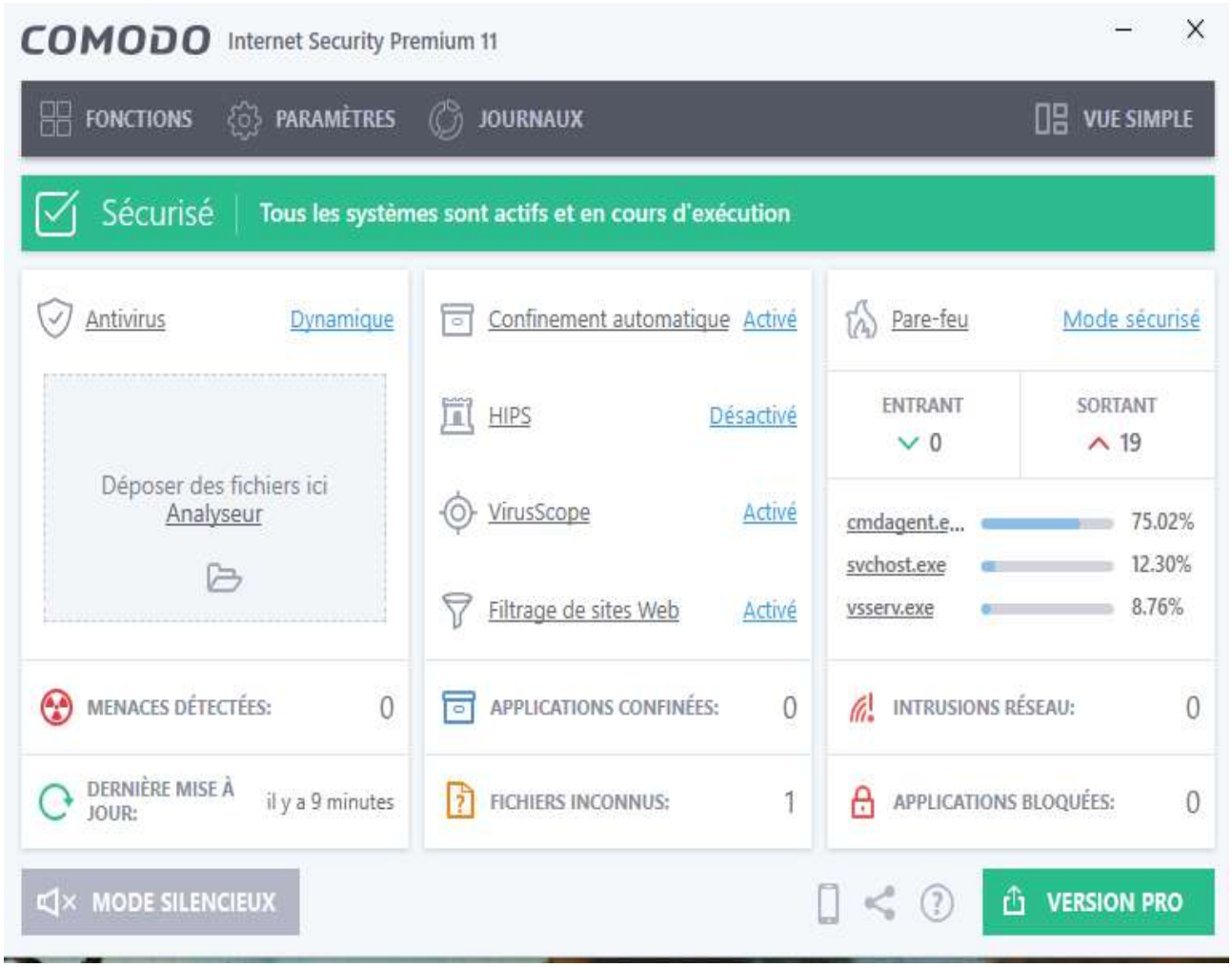
Table des matières

Partie 1 - Installation de Comodo Internet Security (CIS)....4
1 Compatibilité du module Comodo Firewall avec d'autres antivirus 4
2 Téléchargement de COMODO Firewall ou de COMODO Internet Security....5
3 Première phase de l'installation....6
4 Poursuite de l'installation 8
5 Etapes suivantes....10
6 Fin de l'installation, après le redémarrage....13
Partie 2 - Configuration de Comodo Internet Security (CIS)....16
7 Fenêtre d'accueil, vue simple et fenêtre des configurations 16
8 Fenêtre d'accueil, vue avancée....18
8.1 Onglets de la barre supérieure....18
8.2 Activation des six modules de la suite Comodo....18
8.2.1 Module antivirus....18
8.2.2 Module « Pare-feu » et ses modes de gestion....19
8.2.3 Module « HIPS »....21
8.2.4 Modules de confinement automatique, du Viruscope et de filtrage des sites Web :. . .22
8.3 Intrusions Réseau....22
8.4 Applications bloquées....22
8.5 Entrant-Sortant - Applications confinées - Fichiers inconnus....22
8.6 Mode silencieux....22
8.7 Onglet supérieur « Fonctions »....22
9 Fenêtre des « Fonctions »....23
9.1 Fonctions générales....23
9.1.1 Lancer une analyse....23
9.1.2 Mise à jour....26
9.1.3 Applications à débloquer....26
9.2 Fonctions du pare-feu dont « Cacher les ports »....25
9.3 Fonctions du conteneur....27
9.4 Fonctions avancées.. ……. 27
10 Onglet « Paramètres »....28
10.1 Paramètres généraux....28
10.1.1 Interface utilisateur....28
10.1.2 Mises à jour....29
10.1.3 Journaux....30
10.2 Pare-feu....31
10.2.1 Paramétrage (Paramètres du pare-feu)....33
10.2.2 Règles des programmes....33
10.2.3 Règles globales....35
10.2.4 Règles prédéfinies....37
10.2.5 Zones réseaux....37

10.2.6 Groupes de ports....38
10.3 HIPS....38
10.3.1 Paramètres HIPS....39
10.3.2 Règles HIPS....40
10.3.3 Règles prédéfinies....41
10.3.4 & 10.3.5 Objets protégés et groupes HIPS....41
10.4 Confinement....41
10.4.1 Paramètres du confinement....41
10.4.2 Confinement automatique....41
10.5 Évaluation de fichiers....41
10.5.1 Paramètres d'évaluation:....41
10.5.2 Groupes de fichiers....39
10.5.3 à 10.5.5 Vous n'avez rien à configurer....42
10.6 Protection avancée....42
10.6.1 Viruscope....42
10.6.2 Analyser les exclusions, contrôle des périphériques, analyse des scripts....42
10.6.3 Divers & 10.6.4 Shopping sécurisé....42
10.7 Filtrage de sites Web....43
11 Fin du paramétrage de la configuration de base du pare-feu....43
12 Sécurisation de la configuration de base du pare-feu....44
13 Configuration de l'antivirus....45
13.1 Protection en temps réel....45
13.2 Analyses....46
13.2.1 Analyse rapide....46
13.2.2 Analyse complète....48
13.2.3 Analyse manuelle....49
Partie 3 - Navigateurs sécurisés et conteneur....49
14 Dragon et IceDragon, les navigateurs sécurisés de Comodo....49
14.1 Installation de Dragon....50
14.2 Installation d'IceDragon....50
15 Utilisation du conteneur....51
15.1 Utilisation d'un programme dans le conteneur....51
15.2 Autres navigateurs placés dans le conteneur....52
15.3 Limitations pour les navigateurs placés dans le conteneur....53
15.4 Réinitialiser le conteneur....53
16 Aménagement d'IceDragon....54
Partie 4 - Migration de la suite au pare-feu - Désinstallation du produit....56
17 Désinstallation partielle (migration) ou totale de la suite ou du pare-feu....56
18 Mesures générales de sécurité 59
Bibliographie....61

Ce premier tutoriel est consacré à l'installation et à la configuration de **Comodo Firewall et de Comodo Internet Security (CIS)**, seule suite *gratuite* et complète du marché ; il s'inspire du manuel d'utilisation de la suite [1], en anglais, et de douze années de pratique ; le second tutoriel [2] « 2/ Gestion sécurisée du pare-feu » vous permettra de choisir entre un bon niveau de sécurité de base, sans intervention ultérieure de votre part, ou des niveaux de sécurité vous permettant un contrôle plus ou moins étroit selon votre degré d'implication dans la gestion du pare-feu.

Ci-dessous la « Vue avancée » de la suite ; la « Vue avancée » du pare-feu, **qui peut être associé à un autre anti-virus du marché,** est identique, à l'exception de l'absence de la première colonne consacrée à l'antivirus :



Comme vous le voyez sur la fenêtre ci-dessus **Comodo Internet Security** est riche en fonctionnalités et comprend :

- **un antivirus** ;

- **Comodo Firewall**, pare-feu particulièrement performant et riche en fonctionnalités, comportant plusieurs modules :

a/ un module pare-feu proprement dit qui contrôle le trafic des paquets d'informations entre votre ordinateur et les réseaux Internet et local ;

b/ un module HIPS (Host Intrusion Prevention System), important, car il complète le pare-feu en surveillant les applications et les fichiers exécutables de l'ordinateur et en empêchant ceux qui seraient malveillants de modifier les paramètres du système ;

c/ un module Viruscope qui vous alerte en cas d'activité suspecte des processus ;

d/ un module de filtrage des sîtes Web ;

e/ un conteneur (sandbox ou bac à sable), où sont automatiquement exécutées les applications inconnues ou douteuses, et dans lequel vous pouvez ouvrir **Facebook, Twitter**, **messagerie et navigateurs avec lesquels vous pouvez alors surfer sur le Web** en demeurant protégé d'éventuels maliciels (malwares).

f/ **un navigateur sécurisé**, Dragon, mouture de Chrome, sécurisée par Comodo en le reliant à ses serveurs Secure DNS qui filtrent les sites malveillants et empêchent les tentatives d'hameçonnage. Vous pouvez également préférer IceDragon, basé sur Firefox, qui offre les mêmes avantages et que vous pouvez installer préalablement ou postérieurement au pare-feu ou à la suite (cf. paragraphe 14).

Partie 1 - Installation de Comodo Internet Security (CIS)

1 Installation isolée du module Comodo Firewall (avec d'autres antivirus):

Bien que la suite complète **Comodo Internet Security** soit de qualité, certains peuvent préférer utiliser le seul pare-feu **Comodo Firewall** avec un antivirus déjà installé sur leur ordinateur. Depuis 2008 nous avons successivement utilisé sans problème le pare-feu Comodo avec les antivirus Avira, Kaspersky, puis récemment Bitdefender et l'avons vu fonctionner normalement avec les antivirus Norton et Avast.

L'installation du pare-feu se fait sans difficulté lorsque l'antivirus est déjà installé

sur l'ordinateur ; par contre, si le pare-feu est déjà installé, les antivirus demandent généralement de désinstaller le pare-feu avant leur installation :

- pour Norton, il suffit de passer outre à sa demande de désinstallation ou, pour Kapersky, à ses deux demandes ; dans les deux cas l'installation de l'antivirus se poursuivra normalement ;

- pour Bitdefender, il faut d'abord désinstaller le pare-feu pour le ré-installer ensuite.

Il est bien évidemment déconseillé d'associer le pare-feu et la suite Comodo à une suite complète de sécurité comportant déjà pare-feu et antivirus.

2 Téléchargement de COMODO Firewall ou de COMODO Internet Security

2.1 Pour la version 04/2020 : choisissez, selon votre préférence, l'un des deux liens ci-dessous ; ***il sera ensuite très facile de migrer d'un programme à l'autre (cf.17.2)***

2.1.1 Lien vers la page de téléchargement de Comodo Firewall

https://personalfirewall.comodo.com/

2.1.2 Lien vers la page de téléchargement de Comodo Internet Security Premium *(Comodo Free antivirus with Internet Security)*

https://www.comodo.com/home/internet-security/free-internet-security.php

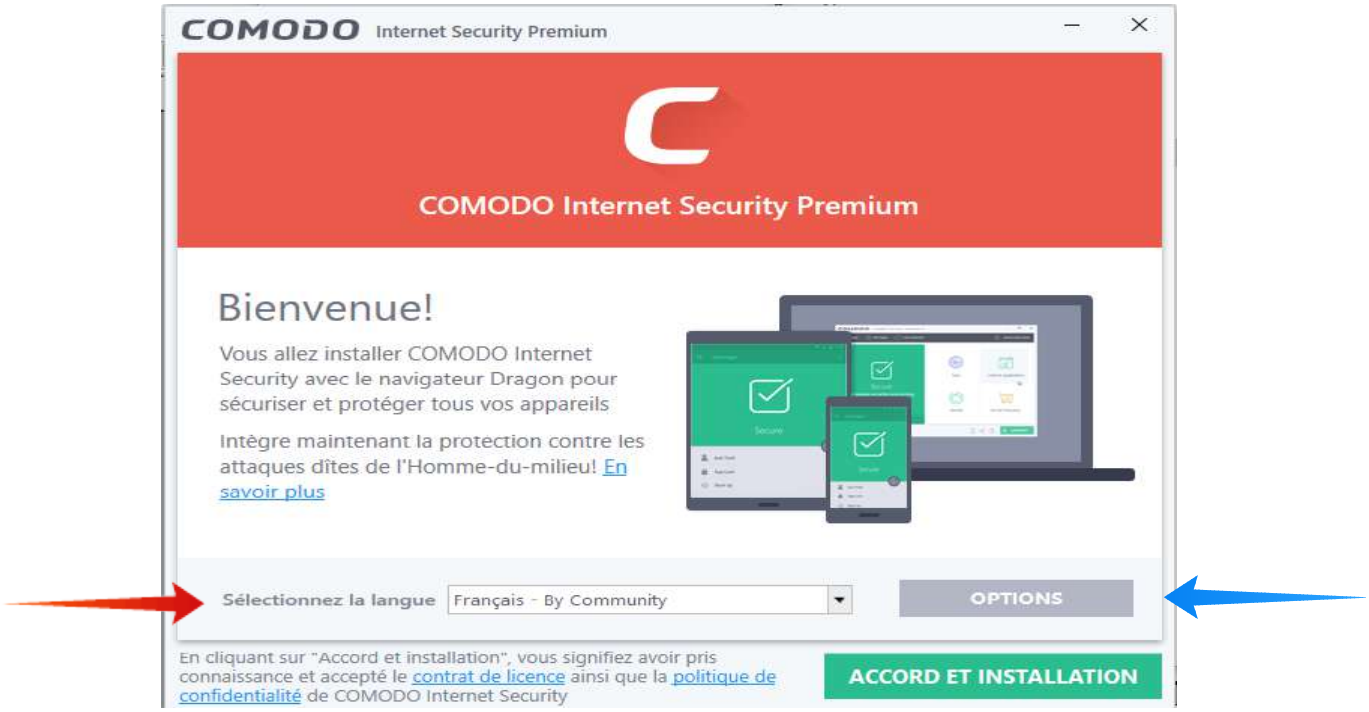
2.2 Pour les versions futures : téléchargez à partir du site de Comodo

Il n'y a souvent que peu de différences d'une version à l'autre de la suite, et la configuration décrite dans ce tutoriel s'applique également aux versions antérieures.

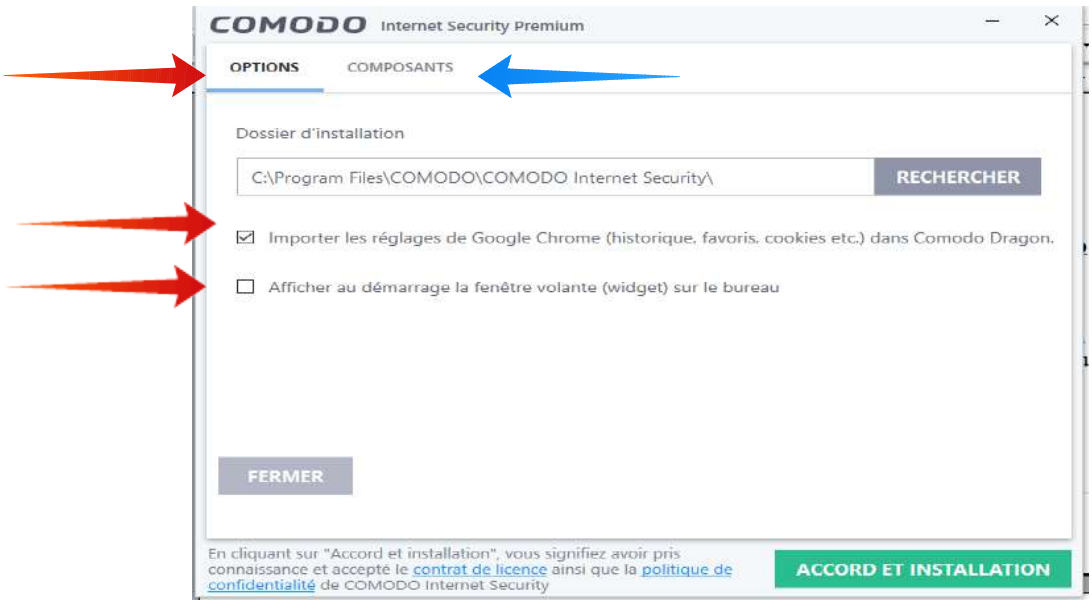
2.3 Note : **dans ce tutoriel nous avons suivi le lien vers la suite complète car les seules différences résident dans l'intitulé « Internet Security Premium » ou « Firewall» et l'ajout du module antivirus pour la suite.**

3 Première phase de l'installation :

- **A partir de l'installateur, téléchargé ci-dessus,** faire un clic droit et choisir « Exécuter en tant qu'administrateur » ; la fenêtre de bienvenue s'ouvre :



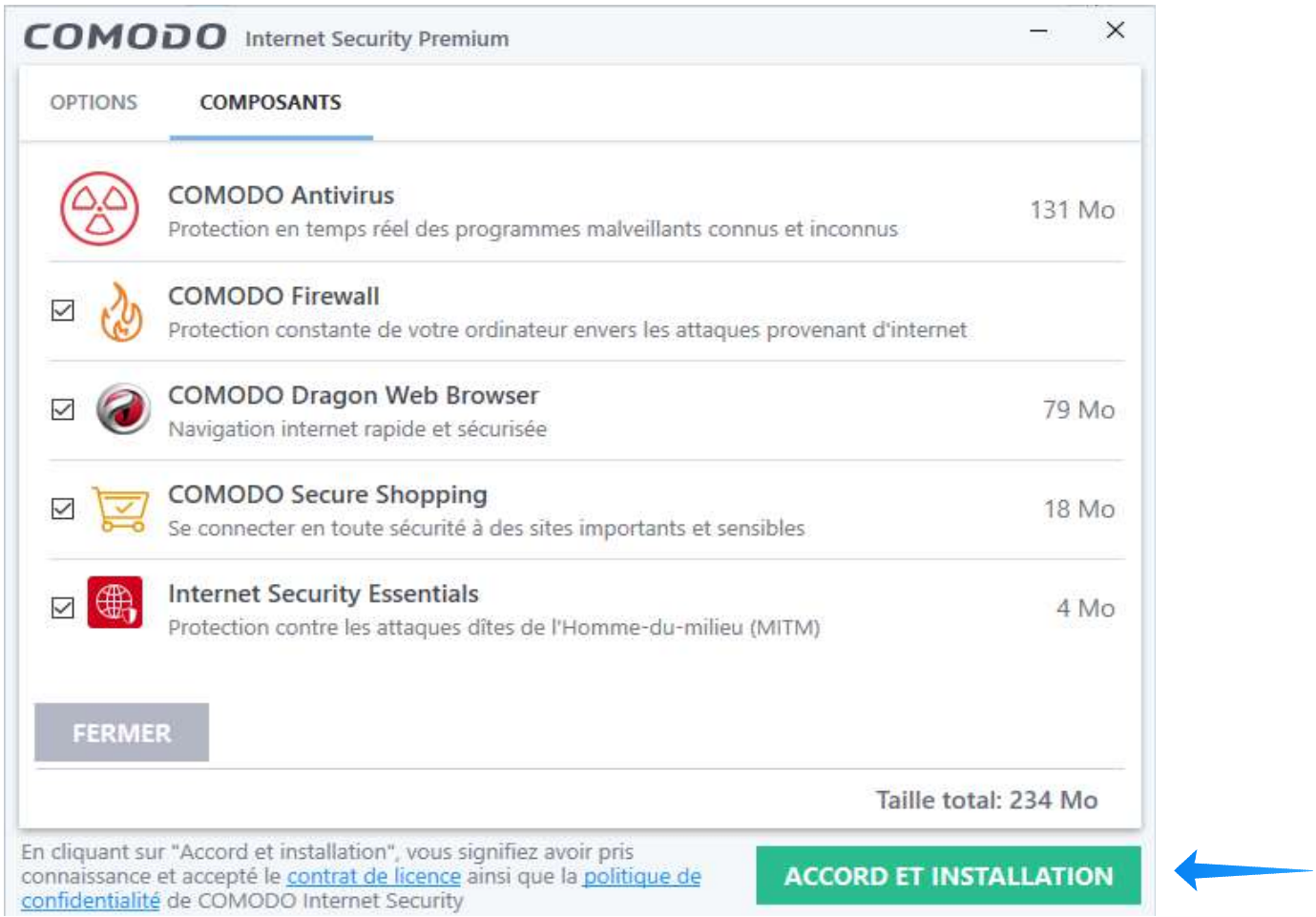
Sélectionner la langue puis cliquer sur « Options » (et non sur « Accord et installation ») ; la fenêtre ci-dessous apparaît :



- Si vous utilisez Chrome vous pouvez laisser coché « Importer les réglages de Chrome » pour le navigateur sécurisé Dragon que vous pourrez ainsi essayer ;

- cocher la seconde ligne pour bénéficier de la fenêtre volante (Widget) et de l'accès aux navigateurs protégés par le conteneur.

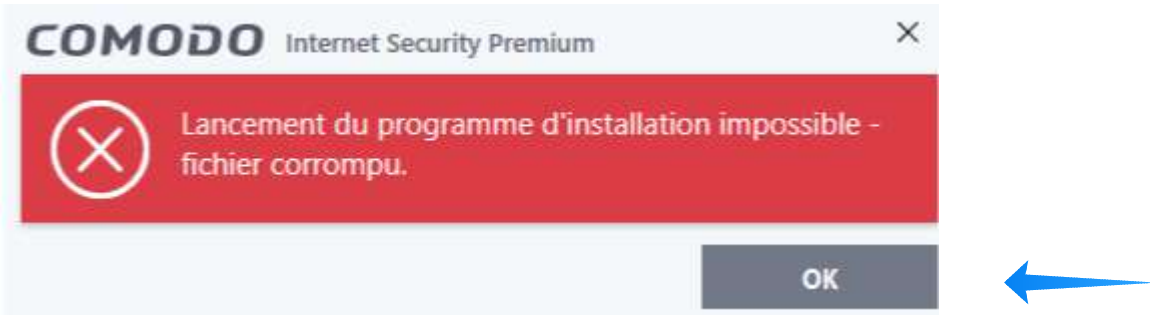
Cliquer ensuite sur l'onglet « COMPOSANTS » :
- Comodo Antivirus ne figure que si vous avez téléchargé la suite, vous pourrez le désinstaller à tout moment (cf. partie 4) ; vous pouvez retenir ou non Comodo Secure Shopping dont nous n'avons pas l'expérience ;
- par sécurité, conservez Comodo Firewall et Internet Security Essentials ;
- vous pouvez conserver Comodo Dragon si vous désirez essayer ce dernier pour surfer sur le Web en étant protégé par le container (cf. partie 3) ;



Cliquer alors seulement sur l'onglet « Accord et installation » : l'installation démarre en restant d'abord pendant 2 à 5 minutes sur 0 %, puis en accélérant :

- **évitez d'interrompre l'installation**, ce qui pourrait créer des problèmes lors d'une future installation ou désinstallation ;

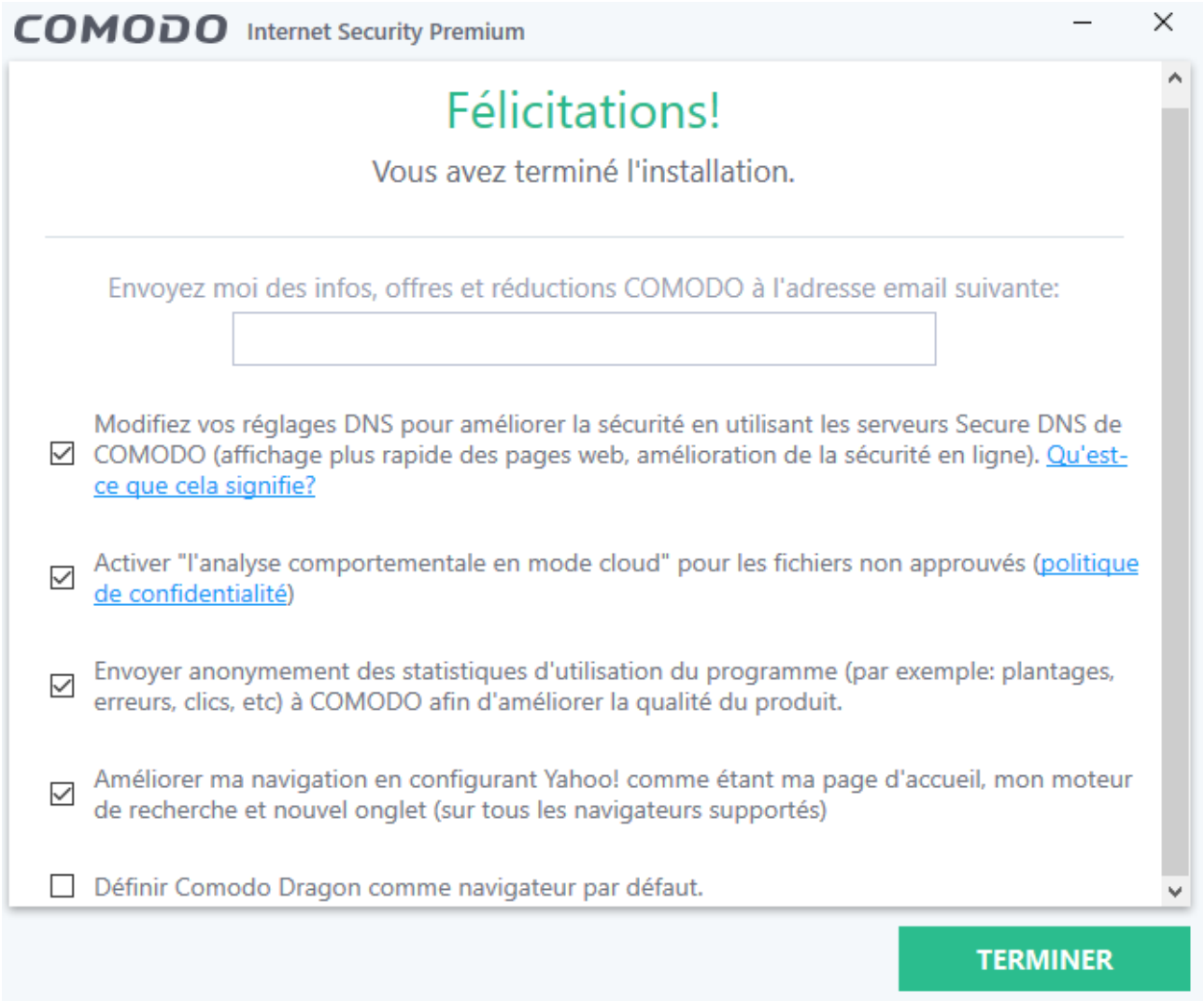
- il arrive parfois que l'installation se bloque avec apparition du message



cliquez sur OK et relancez l'installation à partir de l'installateur ; celle-ci reprend à partir du point de blocage et se termine normalement en quelques minutes.

4 Poursuite de l'installation :

En général, sans qu'il soit besoin de cliquer sur « Terminer », apparaît à la fin de la phase précédente la fenêtre de « Félicitations » ci-dessous où vous pourrez, si vous le désirez, mentionner votre adresse mail avant de retenir certaines options :



- Cette fenêtre propose cinq options, dont les deux premières sont d'importance car elles assurent le fonctionnement sécurisé optimal du pare-feu :

- la première option permet l'envoi des demandes d'adresses DNS sur les serveurs Secure DNS de Comodo qui filtrent les sites Web malveillants jouant ainsi un rôle essentiel dans la protection de votre navigation (cf.14) ;

- la seconde active l'envoi des fichiers non approuvés à Comodo pour analyse

comportementale en mode cloud. Le Centre Comodo testera les fichiers pour déterminer s'ils sont malveillants ou non et les traitera de manière appropriée ;

- la troisième vous propose de participer à l'amélioration du produit ;

- les deux dernières proposent de retenir ou non Yahoo comme page d'accueil de votre moteur de recherche et Comodo Dragon comme navigateur par défaut :

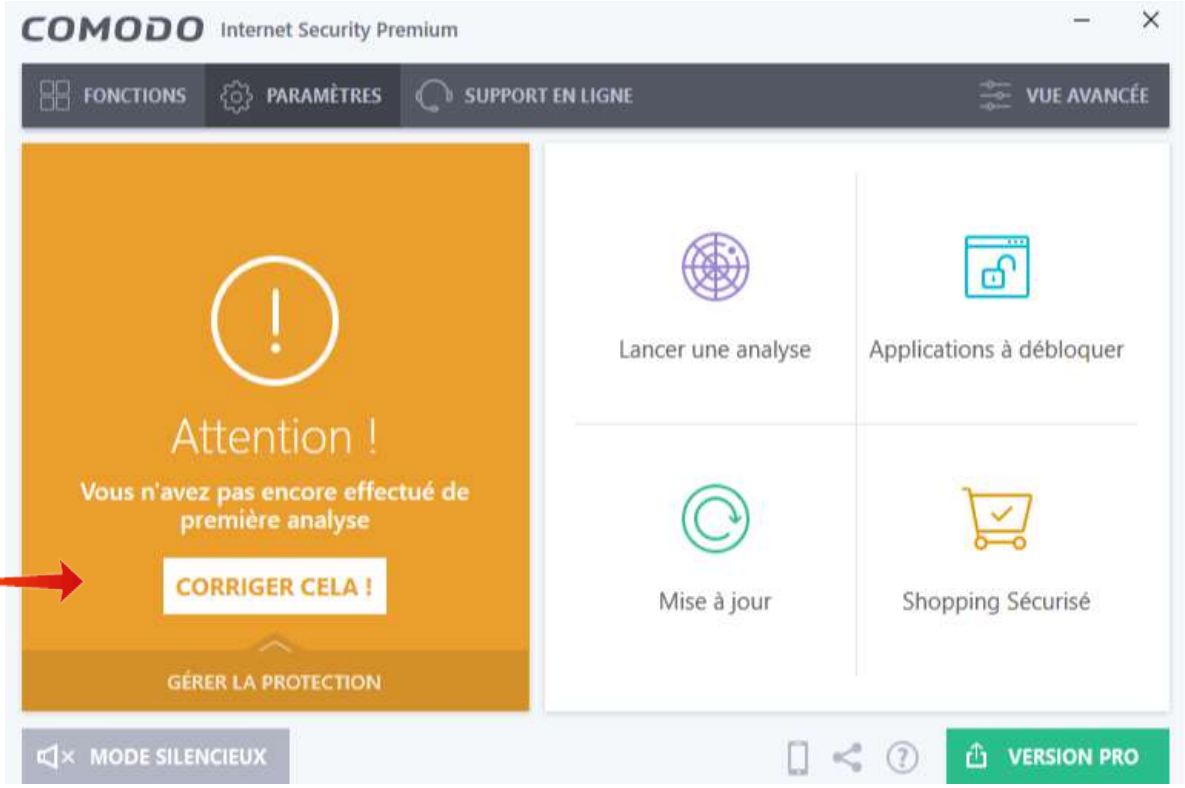
Après avoir retenu les deux premières options essentielles et avoir effectué votre choix pour les trois suivantes, validez en cliquant sur l'onglet « Terminer » : plusieurs fenêtres s'ouvrent alors permettant de passer aux étapes suivantes.

5 Etapes suivantes:

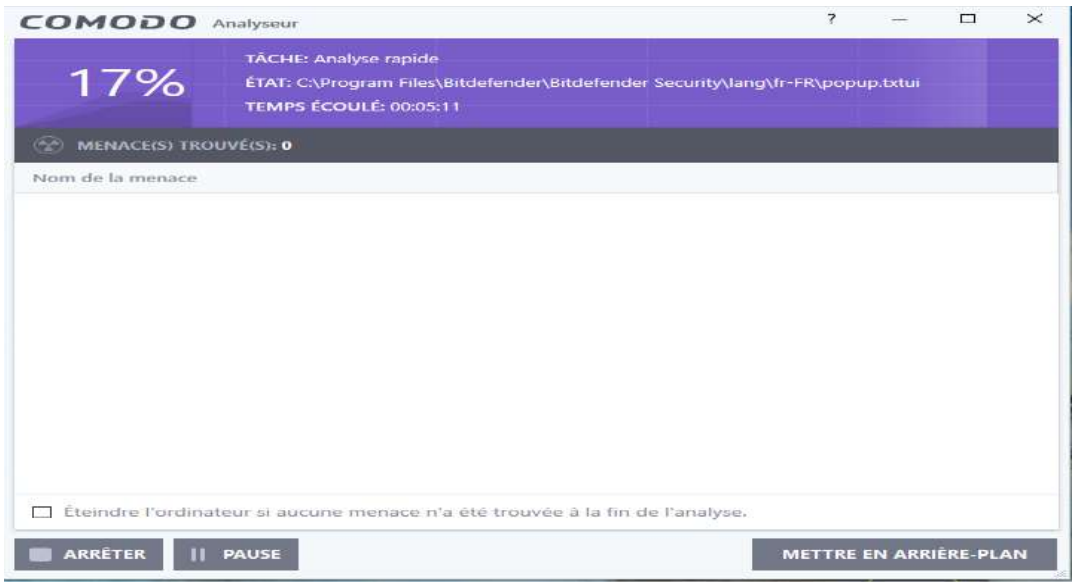
5.1 Apparition à droite de votre écran de la fenêtre mobile (widget) ci-dessous :

La mention « Attention » est sur fond orange, car une analyse rapide est nécessaire ; n avant-dernière ligne, **l'accès dans le conteneur aux navigateurs Dragon, Firefox et Internet Explorer, et, en dernière ligne, à Twitter et Facebook**.

5.2 Demande de première analyse : (ou équivalent pour le pare-feu isolé))



5.3 Immédiatement, ou après avoir cliqué sur « Corriger cela », démarre le téléchargement des signatures virales (6 minutes environ) , puis l'analyse rapide (2 minutes environ) (pour la suite complète seulement) :



A la fin de l'analyse virale (100 %) apparaît le nombre d'éventuelles menaces détectées.

5.4 *Avant le redémarrage ou ultérieurement en cours d'utilisation demande très importante pour la configuration du pare-feu* (cf. [2] 5.2)

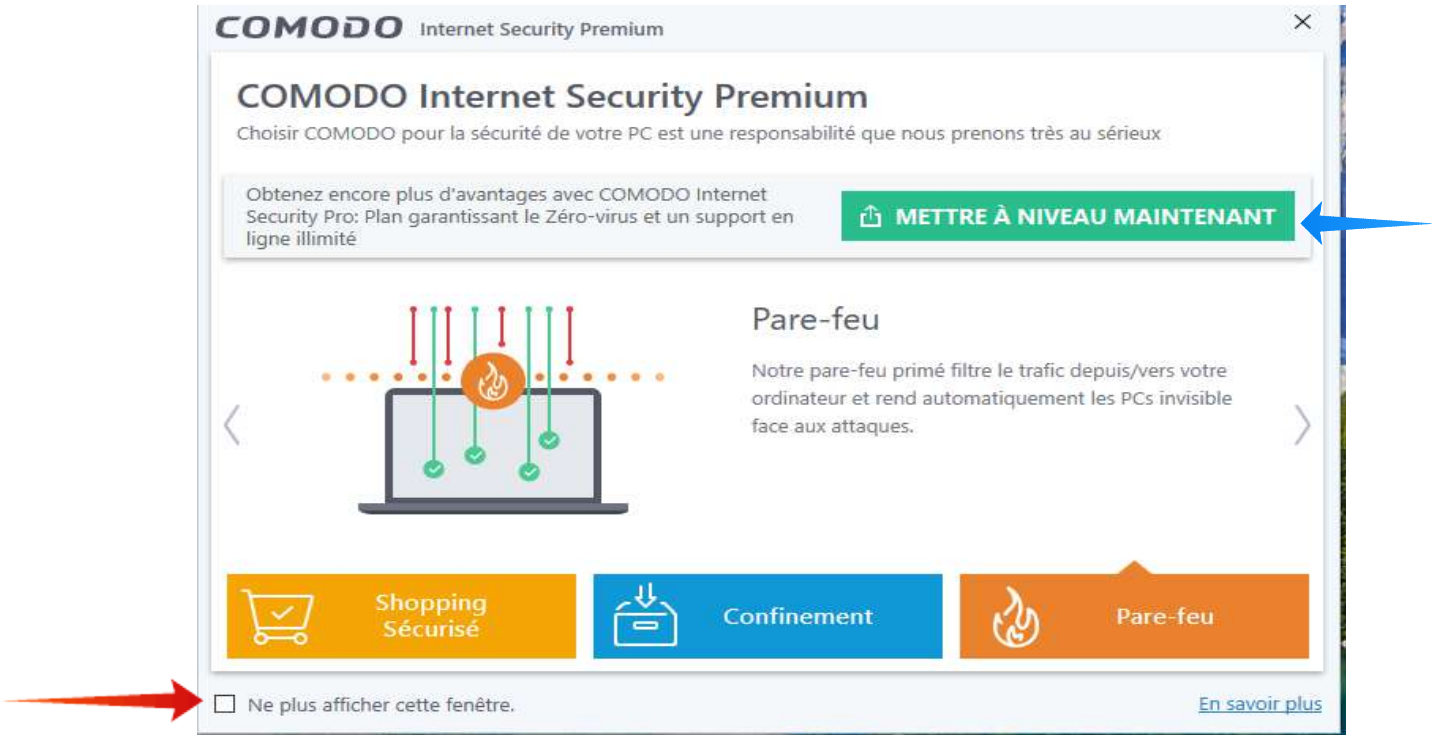
Répondez en fonction de votre localisation ; la case du bas est décochée par défaut, laissez-là ainsi. Ne la cocher que si vous êtes expérimenté et désirez gérer vous-même les réseaux.

5.5 Demande de redémarrage

Vous pouvez redémarrer maintenant ou reporter le redémarrage à 30, 60 minutes ou 4 h :

6 Fin de l'installation, après le redémarrage

6.1 Proposition de mise à niveau vers la suite payante



Vous pouvez **soit choisir « Mettre à niveau maintenant » vers la version payante Pro**

Pour 17,99 $ la version PRO bénéficie exactement du même logiciel, mais avec une assistance illimitée en anglais, une indemnité de 500 $ pour le cas où votre ordinateur serait contaminé et ne pourrait pas être désinfecté par les techniciens de Comodo, une capacité de stockage en ligne de 50 GB, et 10 GB de connexion Wifi sécurisée ;

ou opter pour la version gratuite en cochant « Ne plus afficher cette fenêtre »

6.2 Proposition de mise à jour de Comodo Dragon ou de Comodo IceDragon

Une telle proposition peut apparaître à tout moment : voir 14.2

6.3 L'icône de la barre des tâches est apparue au moment du redémarrage

un clic droit sur le menu déroulant de l'icône permet :

- de choisir les modes de fonctionnement des différents modules : **à ce stade choisissez « Dynamique » pour l'antivirus, « Mode sécurisé » pour le pare-feu et le module HIPS, « Activé » pour le confinement automatique, Viruscope et le filtrage des sites Web ;** nous déterminerons en 8.2 si ces choix sont les plus pertinents en fonction de vos objectifs, et méritent d'être confirmés, ou doivent être modifiés ;

- de passer au mode silencieux lors des jeux ;

- de sélectionner la fenêtre « Vue avancée » et la fenêtre mobile ci-dessous, ainsi que l'affichage des divers volets (dont celui des navigateurs) de celle-ci

- ou de quitter : ***attention cela ferme le pare-feu*** ;

6.4 la fenêtre mobile (widget) indique maintenant que COMODO est sécurisé

Note : en avant dernière ligne les navigateurs Firefox, IceDragon et Internet Explorer.

La fenêtre mobile et la vue avancée de le fenêtre d'accueil (en 8) **sont essentielles à la surveillance du pare-feu ; la fenêtre mobile permet** :

- sur la 1ère ligne, sous COMODO : d'accéder à l'une des fenêtres d'accueil (clic sur la maison dans la barre colorée) et de suivre l'état du pare-feu: **« Attention » (orange), « Menacé » (rouge)** ; **« Sécurisé » (vert), « Mode silencieux » (bleu)**

un double clic sur « Attention » ou « Menacé » ouvrira la fenêtre appropriée à l'action à entreprendre immédiatement ;

- sur les deux dernières lignes, **d'accéder directement au bureau virtuel** dans lequel vous pourrez ouvrir **vos navigateurs vers le Web, notamment Dragon et Firefox,** enfin **Twitter et Facebook,** en demeurant à l'abri de l'incursion d'éventuels pirates ;

- sur les lignes intermédiaires, d'accéder à diverses fonctions, dont **« Applications bloquées »** (et non débloquées), (cf. 12.2.4) ;

L'installation est désormais achevée, nous conseillons d'entreprendre sans tarder la configuration du pare-feu : les choix que vous retiendrez vous orienteront soit vers une gestion automatique sans intervention de l'utilisateur, soit vers une gestion plus ou moins personnalisée selon votre degré d'implication.

En **cliquant sur la petite icône en forme de maison, en haut à gauche, de la fenêtre mobile ci-dessus** on ouvre la vue simple ou la vue avancée de la fenêtre d'accueil (un clic, en haut à droite, permet de passer de l'une à l'autre), **vue avancée à partir de laquelle on débutera la configuration.**

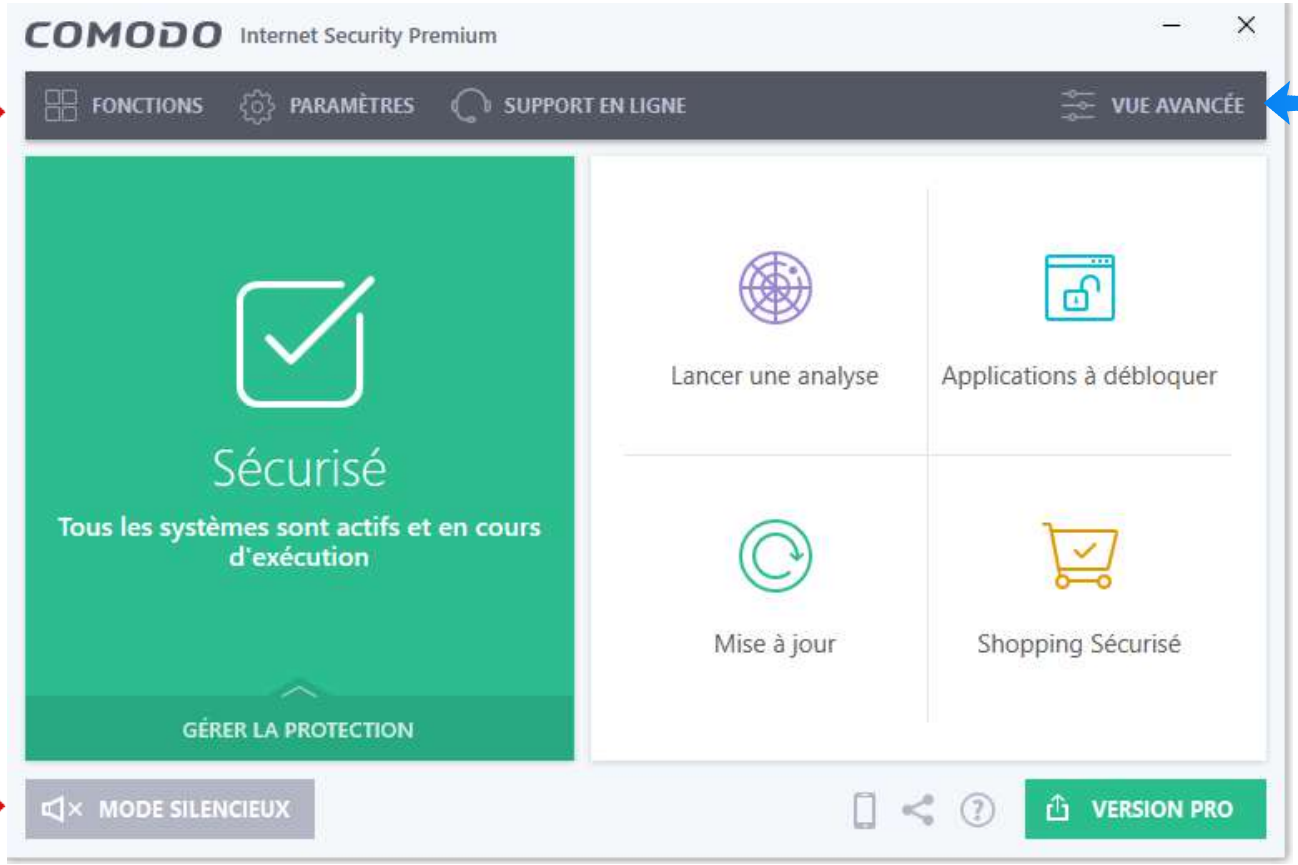
Partie 2 - Configuration de Comodo Internet Security (CIS)

7 Fenêtre d'accueil, vue simple et fenêtre des configurations :

7.1 Les onglets de la barre supérieure permettent d'accéder aux fonctions, aux paramètres, au support en ligne, ainsi qu'à la vue avancée de la fenêtre d'accueil, véritable plate-forme d'orientation du pare-feu ;

7.2 L'onglet « Mode silencieux » permet de ne pas être dérangé par une éventuelle alerte (mode jeu) ;

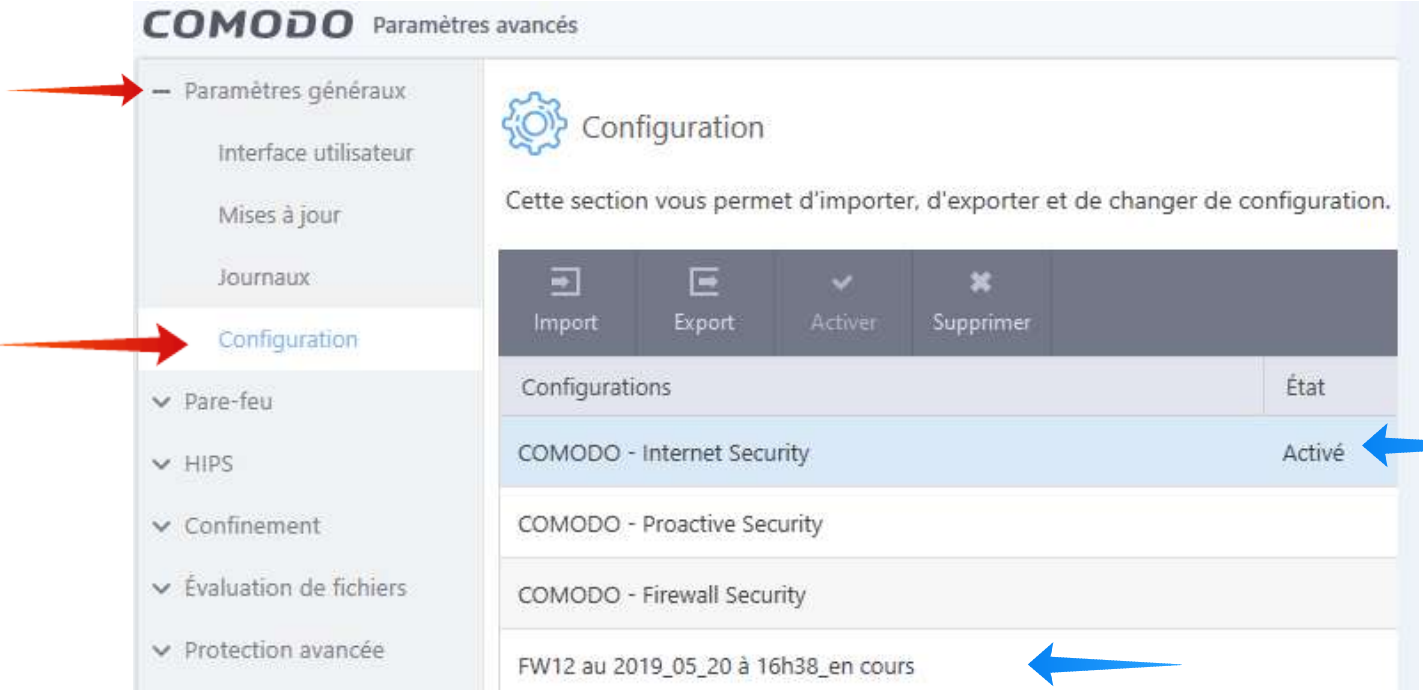
7.3 Les pavés conduisent à différentes fonctions que nous retrouverons dans d'autres fenêtres ;



7.4 Fenêtre des configurations (Paramètres\Paramètres généraux\Configuration)

A partir de la fenêtre des configurations de la page suivante, obtenue en suivant le chemin mentionné dans le titre ci-dessus, nous vous conseillons vivement, **avant de**

paramétrer la configuration, à la fin de celle-ci et, plus tard, lorsqu'un certain nombre de règles auront été activées, de faire un clic droit sur la configuration activée afin de l'exporter : ces configurations exportées constitueront autant de points de restauration disponibles, vous évitant, en cas de problème, de reprendre en totalité la configuration ou de réinstaller le logiciel.



- cliquez droit sur la *configuration activée*, un menu propose alors : Import, Export, Activer, Supprimer ;

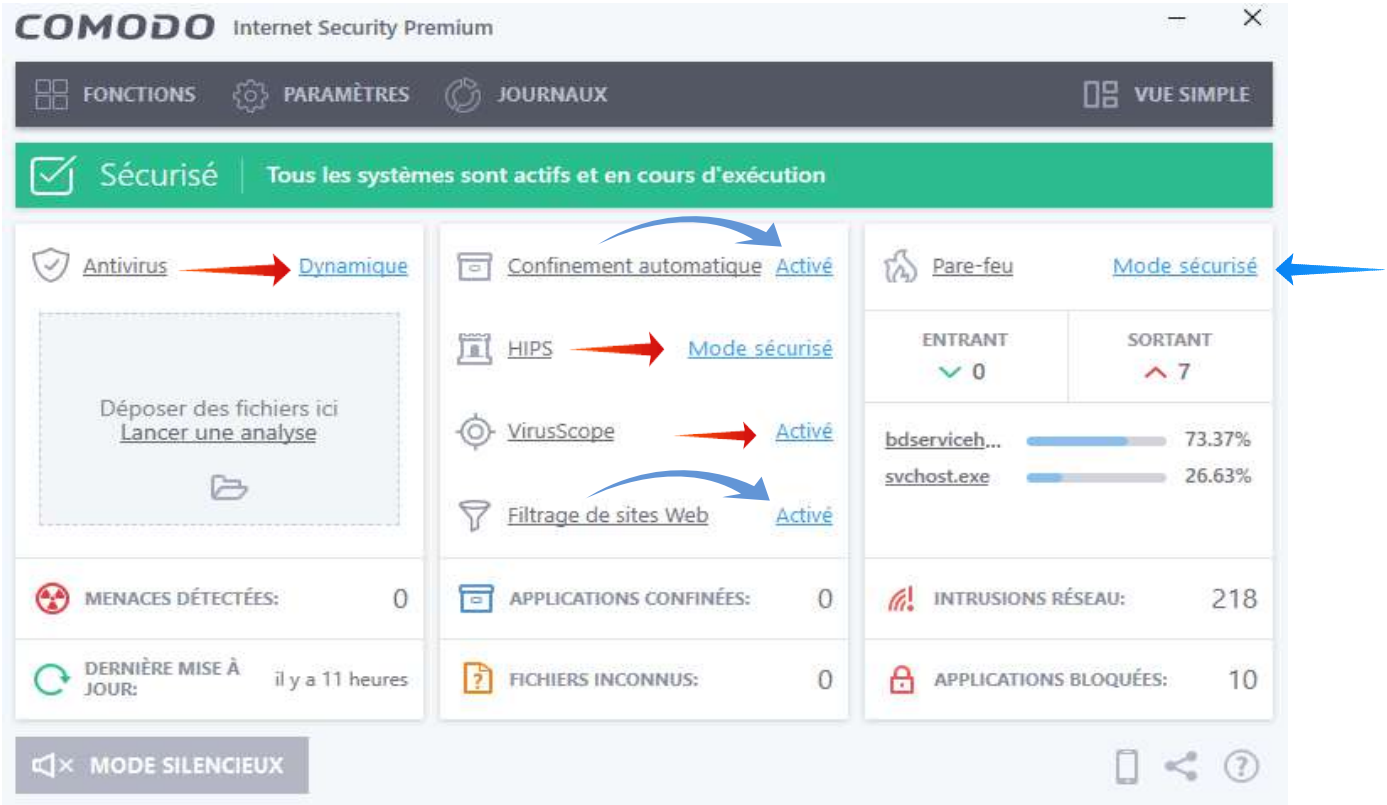
- exportez la configuration activée que vous intitulerez par exemple « Fw12 cfg de départ le ... » vers un dossier de sauvegarde que vous aurez créé sur votre ordinateur ;

- puis, à partir de ce dossier, importez-la dans la fenêtre « Configuration » en l'intitulant par exemple « Fw12 cfg en cours à dater du ... », enfin activez-la : *vous pourrez désormais paramétrer et travailler avec cette configuration,* les trois configurations d'origine resteront ainsi disponibles pour créer de nouvelles configurations en cas de besoin ;

Nous allons désormais passer sans tarder à la configuration du pare-feu, car celui-ci doit déjà être en train de travailler ; nous aborderons la configuration de l'antivirus en 13.

8 Fenêtre d'accueil, vue avancée

Cette fenêtre d'accueil constitue la plaque tournante de la gestion de CIS.



8.1 Onglets de la barre supérieure : ces onglets permettent d'accéder aux fonctions, aux paramètres, et aux journaux, particulièrement développés et précieux.

8.2 Activation des six modules de la suite Comodo : activez-les, à ce stade, comme ci-dessus, s'ils ne l'ont déjà été à partir de l'icône de la barre des tâches :

8.2.1 Module antivirus : colonne de gauche (cette colonne est absente dans la version Firewall isolé) : (cf. paragraphe 13)

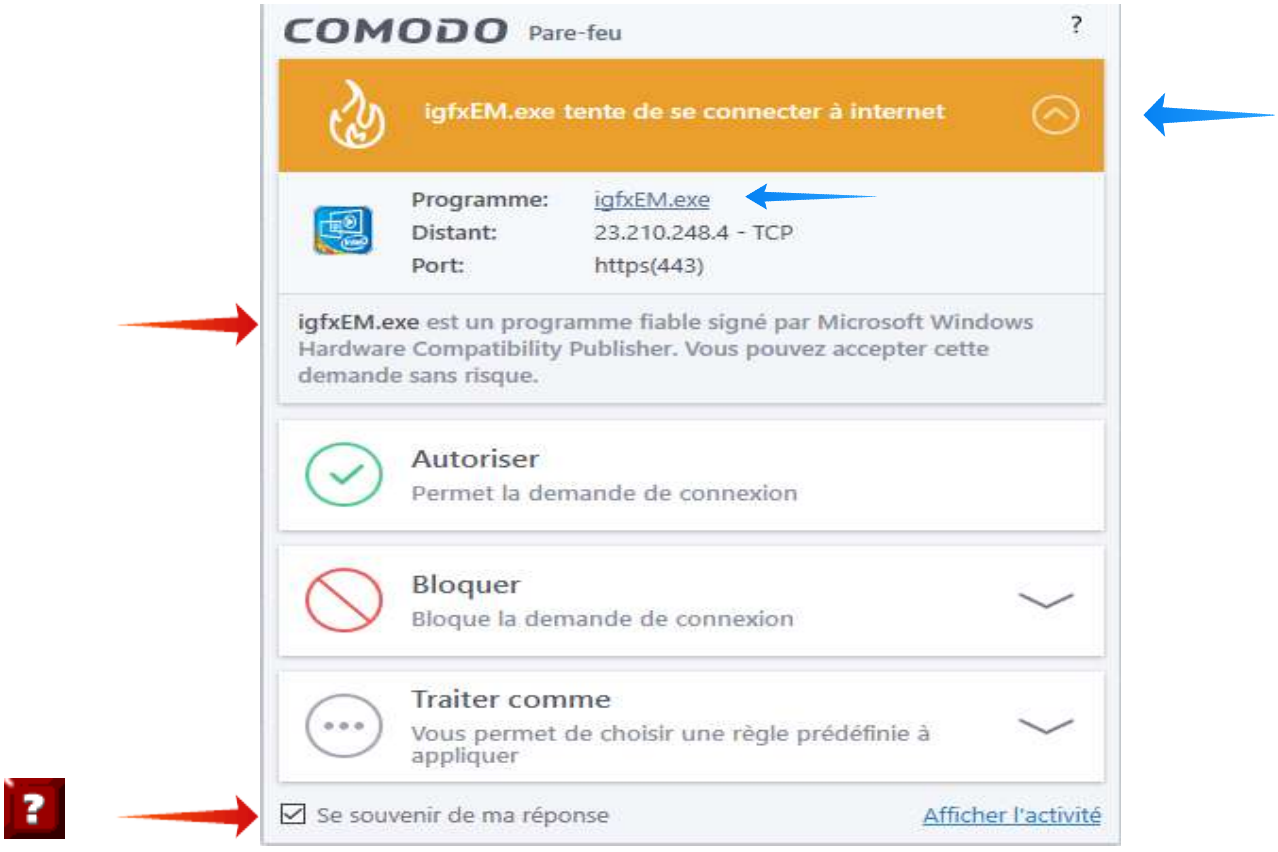
- **Choisissez l'option « Dynamique »** ;

- **Dernière mise à jour** : si la dernière mise à jour est trop éloignée, cliquez pour mettre à jour la base des signatures virales ;

8.2.2 Module « Pare-feu » et ses modes de gestion (en haut, à droite de la fenêtre de la page précédente): un clic gauche déroule un menu qui propose :

- ***« Bloquer tout »*** que l'on utilisera pour bloquer tout le trafic, lors de l'intrusion d'un virus, afin d'empêcher sa diffusion avant qu'il ne soit détruit ;

- ***« Mode personnalisé »*** : dans ce mode le pare-feu traite une application qui tente de se connecter selon les règles déjà spécifiées par l'utilisateur ; en l'absence de règle spécifiée le pare-feu envoie systématiquement une alerte (voir ci-dessous) à l'utilisateur qui décidera si la demande doit être autorisée, bloquée ou traitée selon une règle prédéfinie :



L'utilisateur est assisté dans son choix :

- par un bandeau jaune (requête saine), orange (requête de dangerosité imprécise à évaluer) ou rouge (requête malfaisante) ;
- par un conseil, ici : « igfxEM est un programme fiable ... » ;
- l'utilisateur peut enfin cliquer sur igfxEM.exe pour obtenir les propriétés de cette application,

Si le conseil n'apparaît pas, cliquez sur le chevron en haut à droite pour le déployer.

Comodo conseille le mode personnalisé aux utilisateurs expérimentés qui souhaitent avoir un contrôle maximal du trafic transitant sur leur ordinateur.

De fait, si l'on suit les conseils des alertes avant d'accorder des autorisations, **le mode personnalisé offre plus de sécurité que le mode dit sécurisé, aussi le conseillons-nous**, pourvu que l'utilisateur souhaite s'impliquer quelque peu dans la sécurité de son ordinateur (cf. 12.2) ;
la création de règles prédéfinies adéquates permettra d'éviter de trop nombreuses alertes (cf. [2] 10.1)

- ***« Mode sécurisé »*** (mode par défaut) :

  - le pare-feu applique de lui-même les règles déjà spécifiées ;

  - en l'absence de règle antérieure le pare-feu autorise le trafic pour tous les composants des applications approuvées comme saines par le Centre Comodo ;

  - l'utilisateur ne reçoit d'alerte que pour les applications qui n'ont pas été approuvées comme saines* ; ce sera alors à vous d'autoriser ou non la demande : si vous connaissez la bonne réputation de cette application et que vous êtes en train de l'installer ou de l'utiliser vous pouvez en général l'autoriser ; cependant la demande peut être l'oeuvre d'un maliciel : **dans le moindre doute n'hésitez pas à bloquer la demande,** il est plus facile de modifier, si nécessaire, une règle de blocage que de réparer les dégâts occasionnés par un programme malfaisant ;

  - note* : ***le nombre d'applications traitées par le Centre Comodo étant très élevé, ces alertes sont rares.***

Le mode sécurisé pourra être retenu par les utilisateurs qui ne souhaitent pas s'impliquer dans la gestion du pare-feu et par les nouveaux utilisateurs qui pourront passer au mode personnalisé, davantage sécurisé, dès qu'ils se sentiront davantage familiarisés avec le pare-feu.

Dans ce mode dit sécurisé les règles « Autoriser » pour les applications considérées comme saines ne sont pas créées par défaut, à moins que vous ne **cochiez la case « Créer des règles pour les applications saines »** au **c**hapitre « Paramètres du pare-feu » (voir 10.2.1), ***ce que nous vous conseillons vivement,*** et qui vous

permettra de consulter les règles en cas de besoin ou de les modifier selon vos préférences (en bloquant par exemple les demandes intempestives d'une application).

- ***« Mode apprentissage »*** : **à proscrire**

  - **ce mode est dangereux,** le pare-feu crée automatiquement des règles « Autoriser » pour **toutes** les nouvelles demandes et n'envoie aucune alerte !

  - éviter d'utiliser ce mode, même quelques instants pour créer des règles au début de certains jeux, car on n'est jamais assuré que toutes les applications installées sur l'ordinateur bénéficient de droits d'accès adéquats au réseau.

- ***« Désactivé »*** : **à éviter** ; si vous désactivez le module pare-feu, n'oubliez pas de réactiver auparavant le pare-feu Windows en mode « Toutes les connexions entrantes bloquées ».

8.2.3 Module « HIPS » :

Un clic gauche déroule un menu qui propose :

- ***« Mode paranoïa »*** :

  - HIPS gère et contrôle tous les fichiers exécutables, à l'exception de ceux que vous avez précédemment estimés sains ;

  - toutefois HIPS n'essaie pas d'apprendre le comportement des applications, même si elles figurent sur sa liste des fichiers approuvés, et ne crée pas automatiquement des règles d'autorisation pour les fichiers exécutables ;

  - HIPS envoie systématiquement une alerte à l'utilisateur qui décidera si la demande doit être autorisée, bloquée ou traitée selon une règle prédéfinie ;

  - ce mode entraîne un nombre très élevé d'alertes, Comodo ne le recommande que pour les utilisateurs expérimentés qui souhaitent exercer une surveillance approfondie de l'activité de leur système ; une réponse inappropriée pouvant conduire à un déséquilibre plus ou moins grave du système, **nous le déconseillons à ceux qui n'ont pas une connaissance approfondie des mécanismes intimes de Windows,**

- ***« Mode sécurisé »*** (mode par défaut) :

- HIPS se familiarise avec le comportement, sur votre ordinateur, des applications approuvées comme saines et leur donne en conséquence les autorisations appropriées ; HIPS crée les règles adéquates correspondantes si la case « créer des règles pour les applications saines », en 10.3.1, a été cochée ;

- HIPS n'enverra une alerte à l'utilisateur que pour les seules applications inconnues ou non approuvées ; celui-ci décidera si la demande doit être autorisée, bloquée ou traitée selon une règle prédéfinie ; HIPS édictera alors la règle appropriée à sa réponse ; au moindre doute n'hésitez pas à bloquer la demande.

Comodo recommande le mode sécurisé pour la plupart des utilisateurs ; ***ce mode réunit les avantages de la sécurité la plus élevée à ceux de la gestion d'un nombre peu élevé d'alertes HIPS*** *;*

- ***« Désactivé »*** : à éviter, à défaut penser à ré-activer le pare-feu Windows en bloquant les connexions entrantes pour les réseaux privés et pour les réseaux publics.

8.2.4 Modules de confinement automatique, Viruscope et de filtrage des sites Web : ces trois modules doivent également être activés ;

8.3 Intrusions Réseau conduit directement au **journal des événements du pare-feu**, particulièrement indispensable pour surveiller les tentatives d'intrusion, l'activité des règles consignées, ainsi que pour tester ces règles ;

8.4 Applications bloquées : à suivre ultérieurement en cours d'utilisation afin de débloquer d'éventuelles applications indispensables (antivirus, etc.) : cf. [2] 8.3 ;

8.5 Entrant-Sortant - Applications confinées - Fichiers inconnus permettront, si nécessaire, de consulter et gérer ces paramètres ;

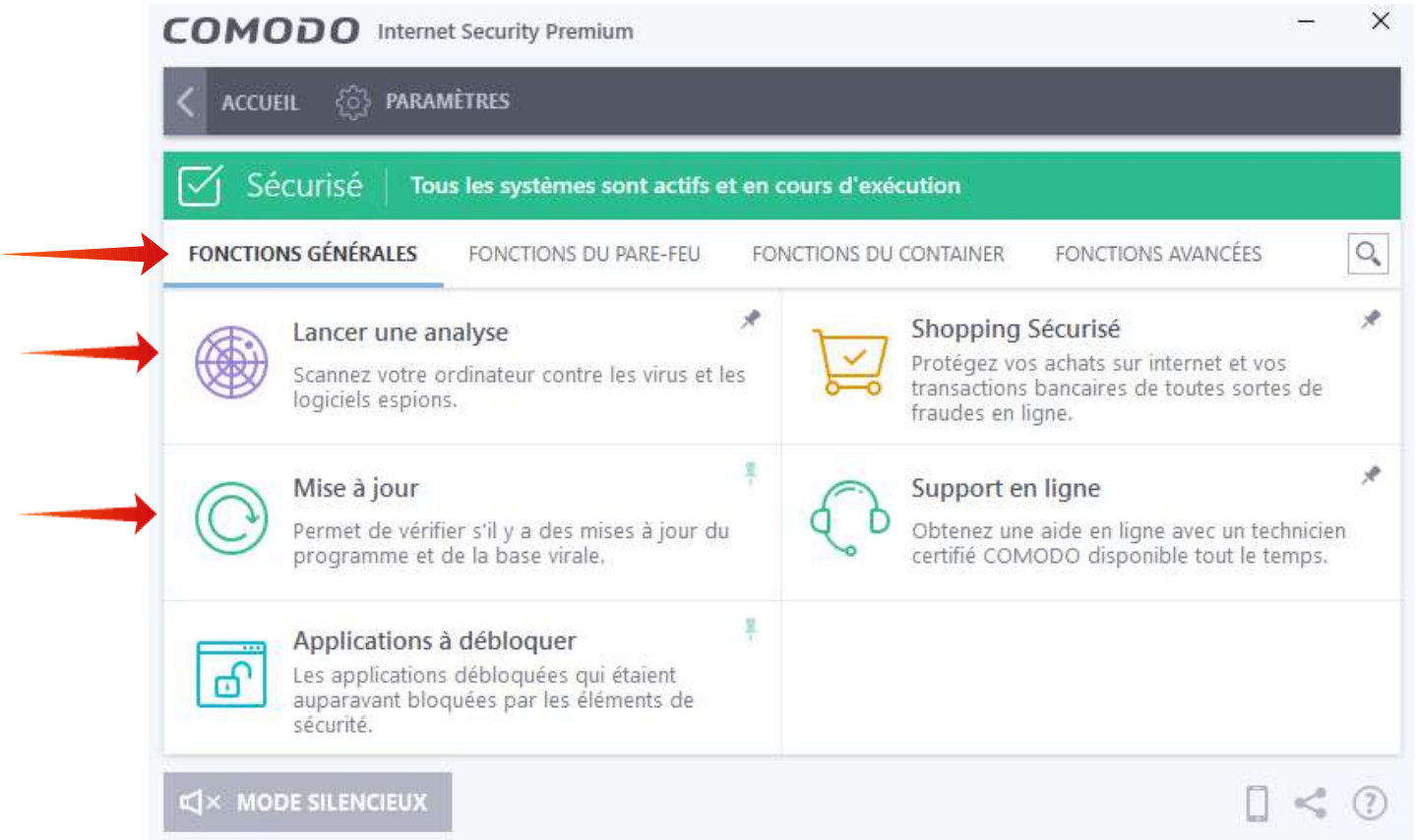
8.6 Mode silencieux pourra être utilisé lors des jeux afin de ne pas être dérangé par une éventuelle alerte ;

8.7 Onglet supérieur « Fonctions » ouvre la fenêtre des fonctions qui suit ;

9 Fenêtre des « Fonctions »

Nous accédons ici aux fonctions regroupées en quatre catégories : voir ci-dessous ;

9.1 Fonctions générales

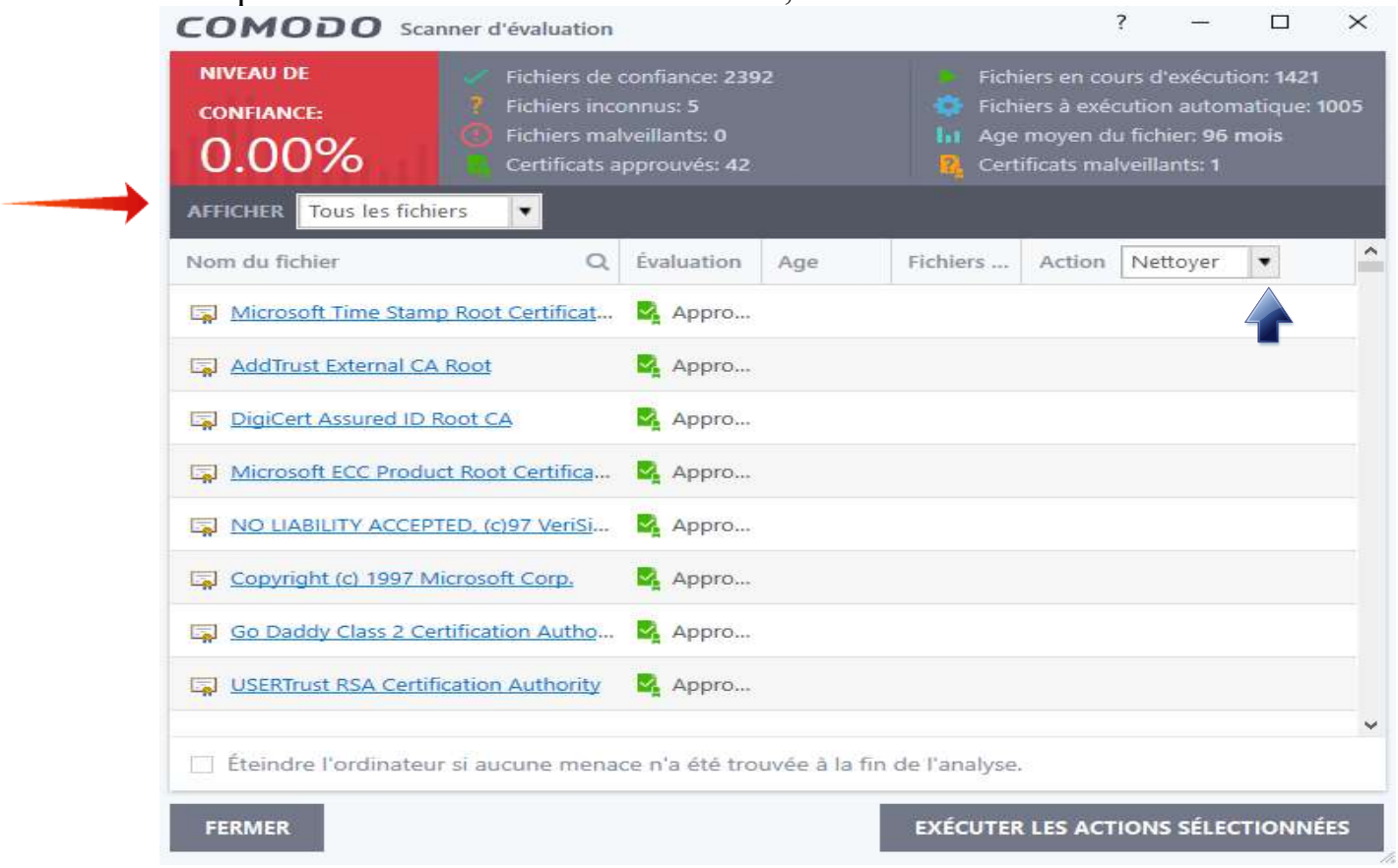


9.1.1 Lancer une analyse

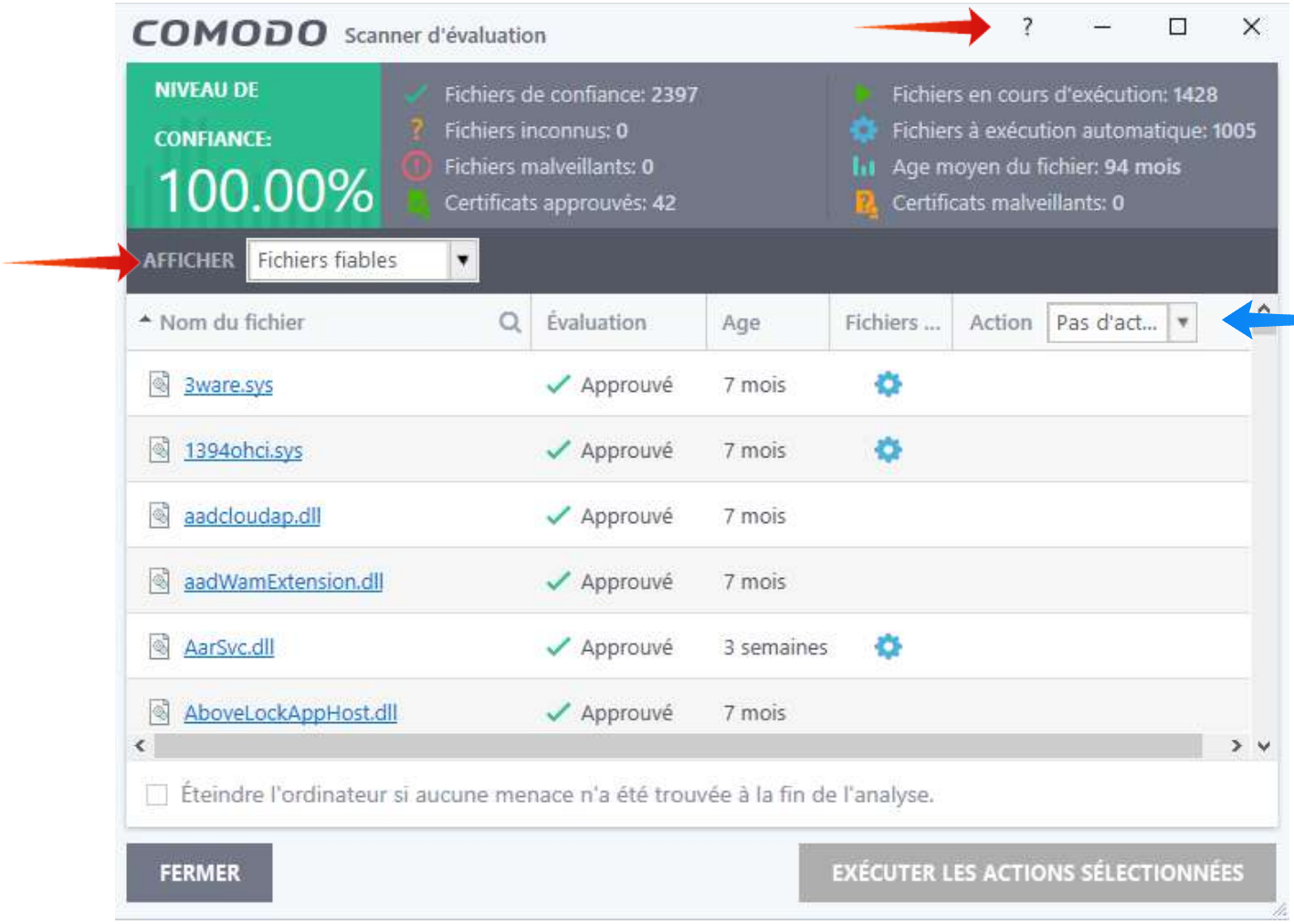
Attention les analyses rapide, complète et personnalisée de la fenêtre de la page suivante sont **des analyses virales** ; **par contre l'analyse d'évaluation ressort de Firewall** : elle évalue les fichiers et certificats présents sur l'ordinateur ;

Lancez dès à présent l'analyse d'évaluation : voir page suivante

Ci-dessous, l'analyse d'évaluation a identifié 2 392 fichiers de confiance approuvés, 5 fichiers inconnus (placés par Comodo dans le conteneur et envoyés pour analyse au centre Comodo) et 42 certificats approuvés ; dans leurs options sécurisées le pare-feu et HIPS créeront automatiquement des règles pour ces applications approuvées. 1 certificat est dit malveillant : dans la case **« Afficher »** on sélectionne **« Certificats malveillants »** ; ici un certificat BitDefender, probablement périmé : avec la flèche vous pouvez opter pour Nettoyer, Pas d'Action ou De confiance ; dans le cas présent on choisira « De confiance » ;



- une nouvelle analyse d'évaluation donne un niveau de confiance de 100 % :



Un clic sur « ? » conduit au paragraphe correspondant du Manuel Comodo en anglais.
Un fichier malveillant aurait pu être identifié en sélectionnant dans « Tous les fichiers » l'item « **Fichiers malveillants** » (et non « Fichiers fiables » comme ci-dessus) ; dans la case « **Actions** » on aurait pu sélectionner « **Nettoyer** » (Clean), ce qui aurait placé le fichier en quarantaine : on se serait alors rendu dans « **Fonctions avancées \ Voir la quarantaine** » où l'on aurait pu restaurer ou détruire ce fichier.

9.1.2 Mise à jour

Dans la fenêtre des « Fonctions générales » de 9.1, lancer maintenant, en une mise à jour unique, la vérification des signatures (virales), de la base des données d'URL pour le pare-feu, des « Recognizers » (fichiers de reconnaissance du comportement des maliciels) qui sont utilisés par le module Viruscope, du programme lui-même, ainsi que le téléchargement de la base de données d'URL ;

9.1.3 Applications à débloquer

Il n'y a rien à paramétrer à ce stade, mais , en cours d'utilisation, il est souhaitable de vérifier qu'un programme important n'a pas été bloqué » (cf. [2] 8.3).

9.2 Fonctions du pare-feu

Il n'y a qu'une seule fonction, la plus importante du pare-feu, à paramétrer dans cette fenêtre : dès l'installation du pare-feu il importe de sécuriser au plus tôt l'ordinateur **en interdisant les connexions entrantes en provenance d'Internet : cliquer sur « Cacher les ports » :**

La fenêtre ci-dessous s'ouvre :

- **Choisissez sans hésitation « Bloquer les connexions entrantes »,** option de loin la plus sûre : cela va entraîner la création par Comodo de règles globales dont l'une

interdit toutes les connexions entrantes à partir d'Internet et rend l'ordinateur invisible à partir du réseau (cf. 10.2.3) ;

- **La seconde option, « Alerte sur les connexions entrantes »**, *beaucoup moins sécurisée*, est à réserver à des cas particuliers comme le « pair à pair » (Peer-To-Peer ou P2P), les sessions de Bureau à distance (Remote desktop) ou certains jeux qui requièrent la visibilité des ports afin de permettre la connexion à votre ordinateur, mais ceci sort du cadre de ce tutoriel.

9.3 Fonctions du conteneur :

- **« Exécuter en virtuel »** permet de placer un programme, **par exemple un navigateur**, dans le container afin qu'il demeure protégé d'éventuels maliciels : cf. paragraphe 15.

- **« Réinitialiser le container »** permet de nettoyer de temps à autre d'éventuelles données contaminées ; cette option peut également être employée lorsque l'accès à un programme situé dans le container devient impossible.

9.4 Fonctions avancées

Ces fonctions avancées seront intéressantes à découvrir ultérieurement, notamment :

- créer un disque de secours, ouvrir le gestionnaire de tâches, afficher les journaux, voir la quarantaine, soumettre des fichiers suspects ;
- et « Nettoyer ce end-point » pour télécharger un programme de nettoyage des ordinateurs infectés.

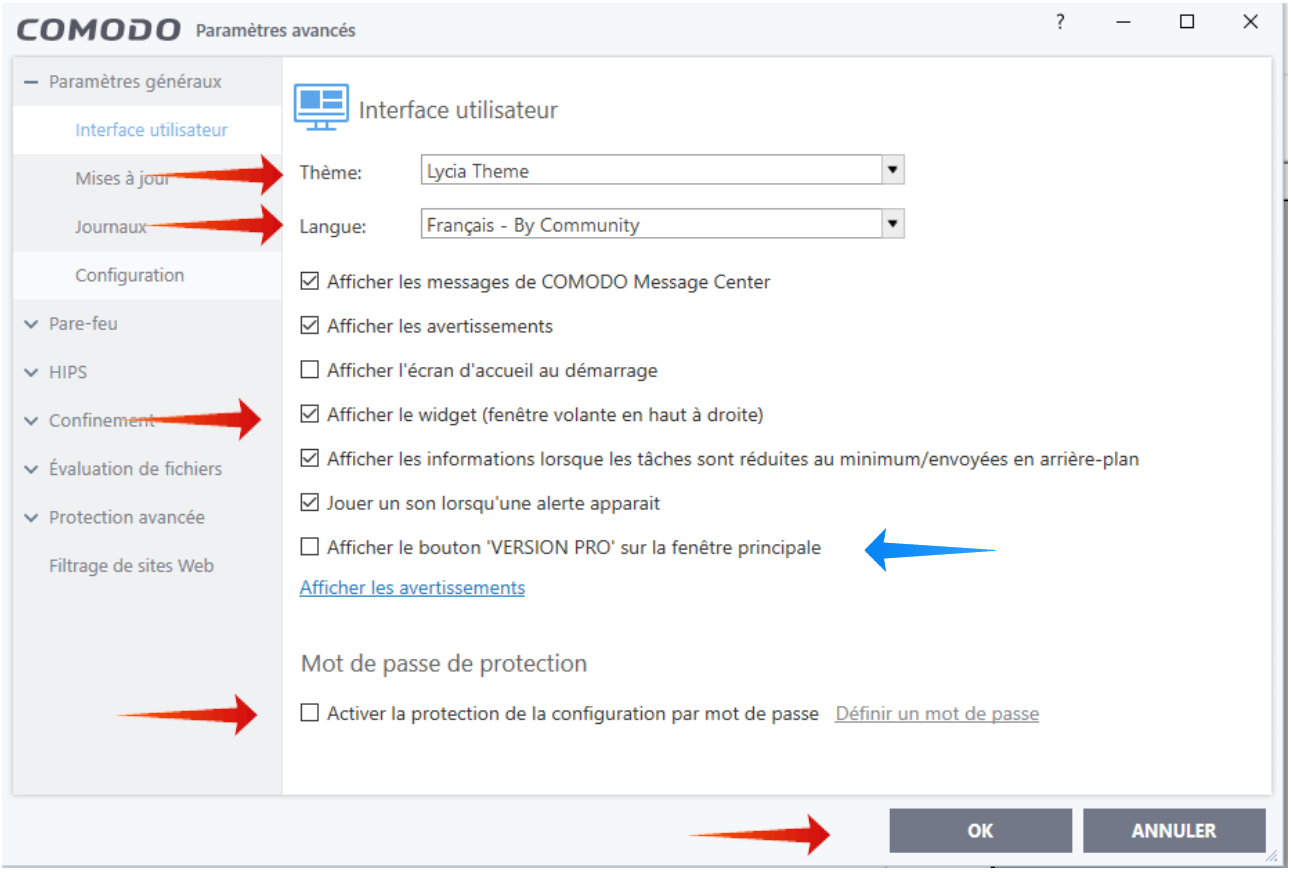
10 Onglet « Paramètres »

Cet onglet conduit aux éléments essentiels qui doivent être configurés.

10.1 Paramètres généraux

10.1.1 Interface utilisateur

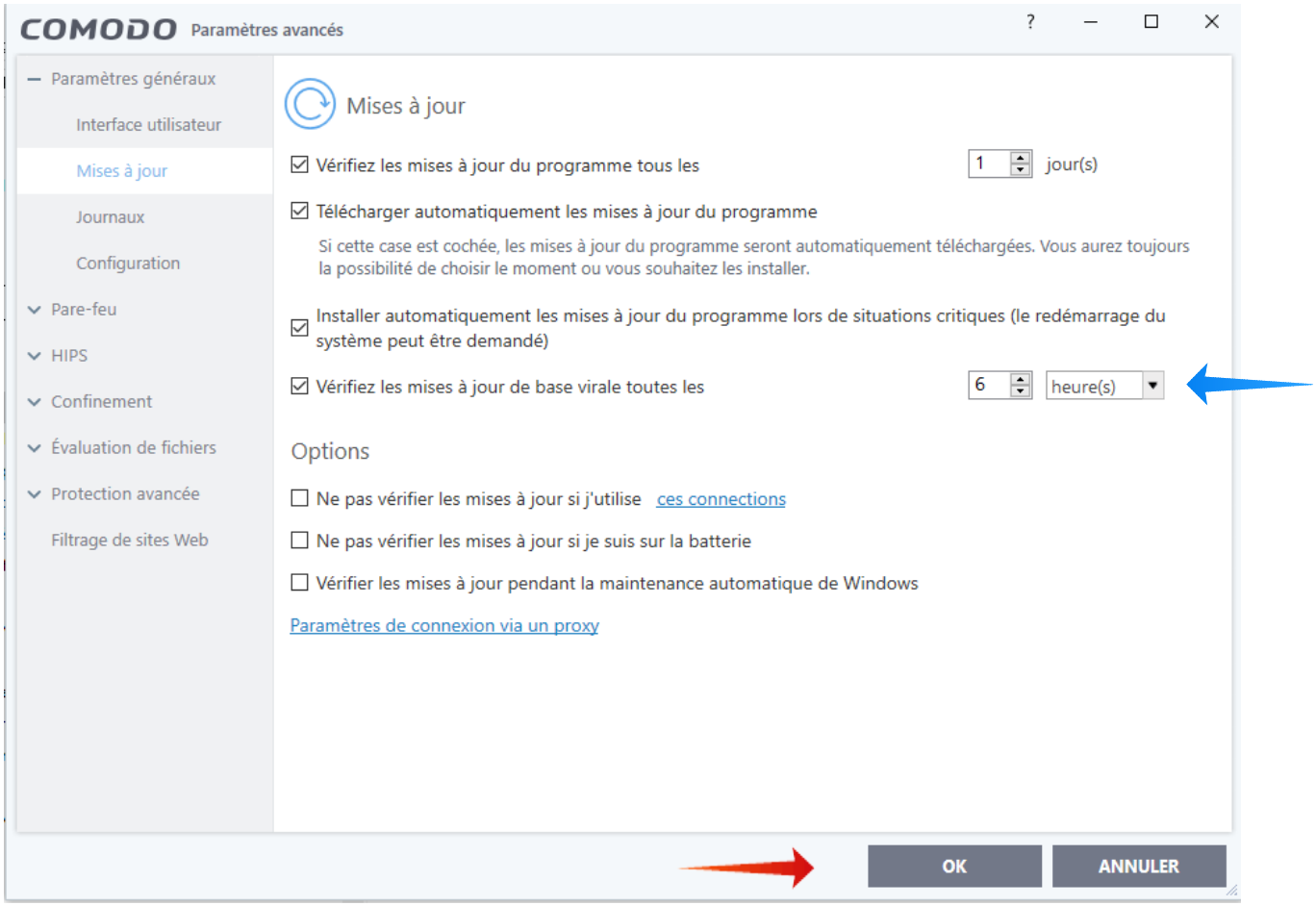
On cochera comme dans la fenêtre ci-dessous :



- « **Lycia Theme** » a été retenu pour les figures de ce tutoriel, les fenêtres obtenues avec quelques-uns des autres thèmes sont parfois différentes ;
- choisir la langue, ici le français ;
- on peut décocher « Afficher la version PRO » ;
- **le mot de passe de protection pourra être activé à la fin de la configuration.**

N'oubliez pas de valider le paramétrage en faisant OK en bas de chaque fenêtre.

10.1.2 Mises à jour



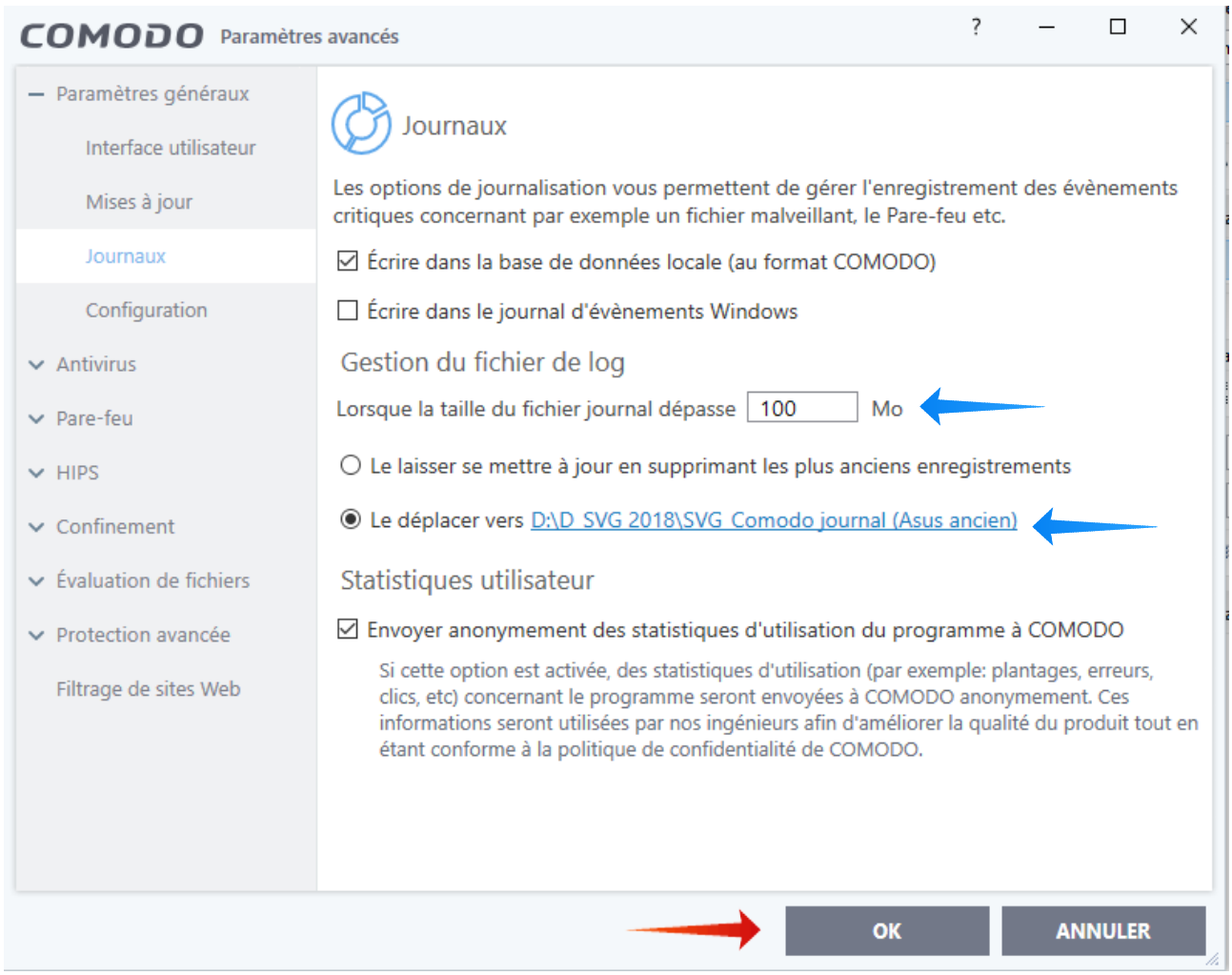
- **dans la fenêtre ci-dessus laissez les trois premières cases cochées** ;

- dans le cas de la suite complète Comodo Internet Security, **renseignez la fréquence des mises à jour de la base virale : passez par exemple de 6 h à 2 h** ;

- si vous êtes sur un ordinateur portable, cochez « ne pas vérifier les mises à jour si je suis sur la batterie » ;

- validez en cliquant sur **OK.**

10.1.3 Journaux



- vous pouvez laisser la première case cochée et la seconde décochée (paramètres par défaut) ;

- pour la gestion du fichier de logs (fichier journal) vous pouvez laisser la taille du fichier à 20 Mo si vous avez peu de place sur votre disque dur, ou l'augmenter ; vous pouvez également déplacer le fichier, par exemple vers un des disques durs où vous avez davantage de place, comme ci-dessus, ce qui permettra de conserver plus longtemps trace des événements les plus anciens pour d'éventuelles consultations,

Pour l'utilisation du Journal des « Evènements Pare-feu » consulter [2] 8.4.2.

10.2 Pare-feu

Votre ordinateur est capable d'établir des connexions afin d'échanger des paquets d'informations avec des ordinateurs du monde entier au travers de ses 65 635 ports. L'acheminement des paquets se fait sur le réseau internet IP (Internet Protocol) situé sur la couche 3 du modèle TCP/IP ; IP fait principalement appel à deux protocoles de la couche 4 de ce même modèle : TCP (Transmission Control Protocol), et UDP (User Datagram Protocol) et, accessoirement, est assisté d'ICMP (Internet Control Message Protocol) et d'IGMP (Internet Group Management Control) : cf. [2] « Gestion sécurisée du pare-feu 1 » pour plus de détails sur le modèle TCP/IP ;

Le rôle essentiel du pare-feu consiste à gérer les demandes de connexions entrantes et sortantes initiées par des applications situées soit sur votre ordinateur, soit à l'extérieur de celui-ci, en fonction des règles d'autorisation ou de blocage, globales et/ou spécifiques, que vous aurez établies en spécifiant notamment les protocoles, destinations et ports concernés.

Gestion des connexions entrantes

- Afin d'établir une connexion entrante un ordinateur extérieur interroge le vôtre afin de voir si des ports sont en attente d'une demande de connexion provenant de l'extérieur ;

- votre pare-feu doit bloquer les connexions entrantes en maintenant les ports de votre ordinateur fermés afin d'empêcher qu'un intrus ne pénètre, et en rendant ces ports invisibles, afin d'éviter que, grâce à un balayage (scan) de ports initié par un pirate, la présence de votre ordinateur ne soit révélée ; **il faut donc éviter, autant que possible, les connexions entrantes.**

Gestion des connexions sortantes

- Une connexion sortante est lancée de l'intérieur de votre ordinateur en direction d'ordinateurs présents sur le réseau Internet ou sur le réseau local, par une application initiée par vous-même ou par une autre application, qu'elle soit saine ou malfaisante ; une fois la connexion établie votre ordinateur peut exporter des données à l'extérieur **ou en importer** ;

- Lors de la demande de connexion à Internet de la part d'une application autorisée, la box initiera l'ouverture d'un port dynamique (de 49152 à 65535) durant le temps de la

session ; port par lequel un intrus pourra pénétrer si l'application autorisée est mal configurée, si elle présente une faille de sécurité non corrigée lors d'une mise à jour ou si elle repose sur un protocole mal maîtrisé au niveau du pare-feu ;

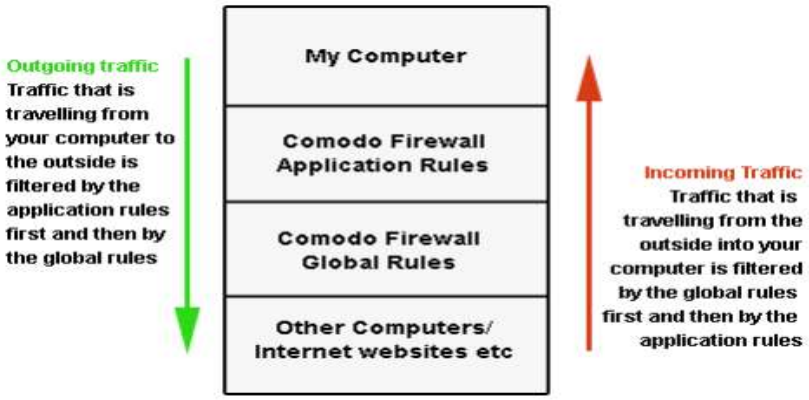
- afin d'assurer une sécurité optimale il est donc souhaitable de n'autoriser des connexions que pour des applications saines et qui vous sont indispensables.

Règles de programmes et règles globales

- 0n distingue des règles et sous-règles de programmes, spécifiques d'applications particulières, et des règles globales s'appliquant à l'ensemble du trafic transitant par votre ordinateur ou s'appliquant à un protocole, un port, un groupe de ports, un ensemble d'applications ;

- le trafic entrant sera d'abord filtré par les règles globales, puis par les règles de programmes concernées ;

- inversement le trafic sortant sera d'abord filtré par les règles de programme appropriées, puis par les règles globales ;



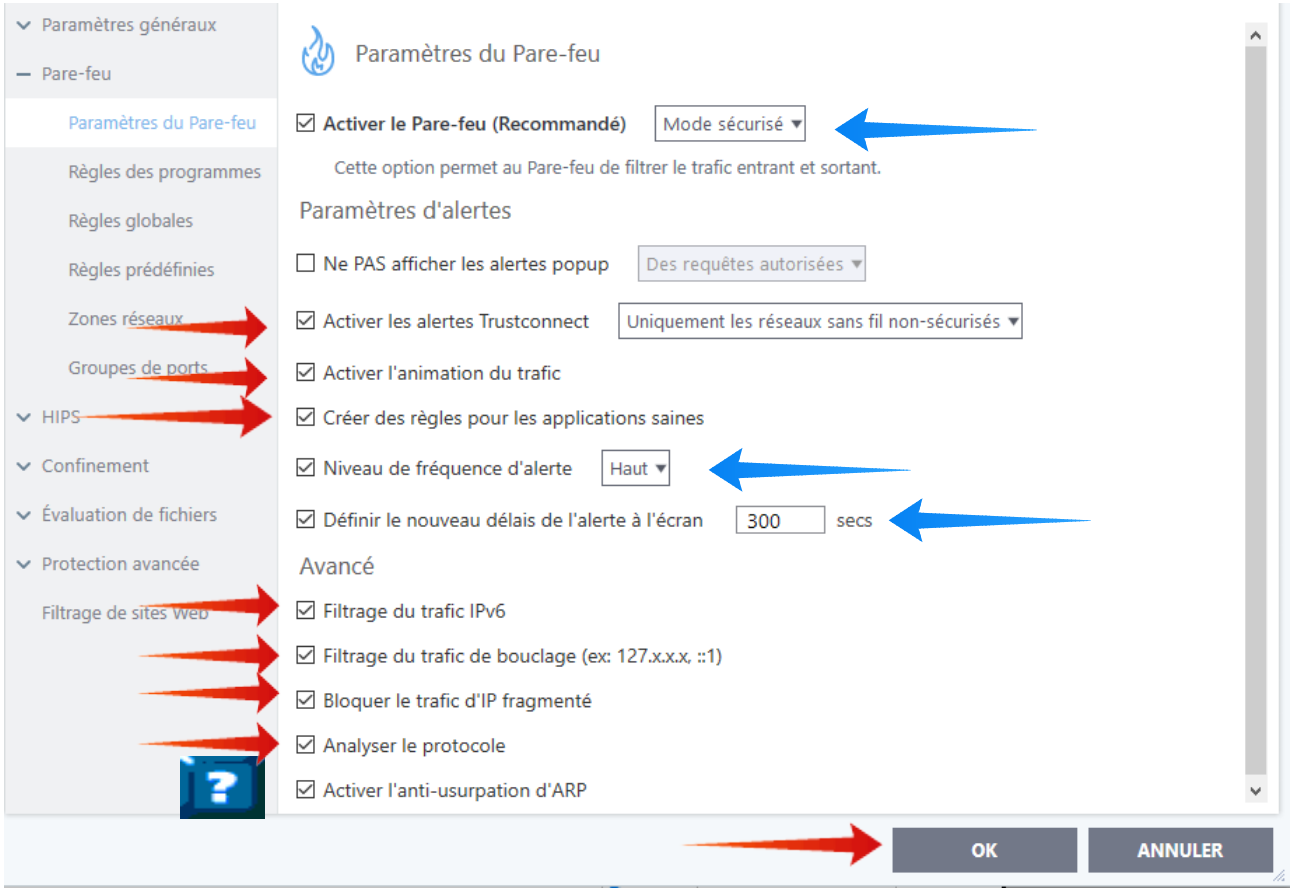
(figure extraite du manuel d'utilisation de Comodo Internet Security)

- à l'intérieur de la fenêtre des règles globales, une règle située en haut de cette fenêtre sera prioritaire sur les règles situées en dessous d'elle ;

- il en va de même à l'intérieur d'une règle de programme pour les sous-règles du dit programme.

10.2.1 Paramétrage (Paramètres du pare-feu) :

Ce paramétrage est décisif ; afin d'assurer au mieux la sécurité de l'ordinateur nous allons configurer le pare-feu comme ci-dessous :



a/ « Activer le pare-feu » en mode sécurisé : on choisira ultérieurement le mode personnalisé en cas de passage au niveau 2 ou 3 de sécurité (cf. [2] 10.3).

b/ Décocher « Ne pas afficher les alertes popup » afin de bénéficier des alertes qui vous informeront de la dangerosité ou non d'une requête de connexion.

c/ Laisser cochées les deux lignes suivantes.

d/ Si vous désirez consulter les règles de programmes appliquées, si vous souhaitez pouvoir éventuellement les modifier, bloquer ou classer en cours d'utilisation, n'hésitez pas à cocher la case « **Créer des règles pour les applications saines** ».

e/ Niveau de fréquence d'alerte

Attention cette option définit non seulement le niveau de fréquence des alertes, mais également, ce qui n'est pas mentionné dans le manuel d'utilisation, **la plus ou moins grande spécificité des règles** qui seront créées par Comodo ;

On évitera à la fois le niveau très haut qui engendre de trop nombreuses alertes, et les niveaux inférieurs qui génèrent des règles autorisant inutilement des ouvertures de ports qui ne seraient pas nécessaires et pourraient être dangereuses : **le choix du niveau haut constitue un compromis équilibré assurant une bonne sécurité et une gestion aisée ;** si vous êtes en mode sécurisé, vous n'aurez, de toute façon, que de rares alertes pour les seules applications inconnues de Comodo : les raisons de ce choix très important sont explicitées en [2] 8.1 ;

f/ Durée de l'alerte à l'écran : porter cette durée de **120 à par exemple 300 secondes,** ceci vous laissera davantage de temps pour répondre à une alerte.

g/ Paramètres de niveau avancé : afin d'améliorer la sécurité :

- **cochez « Filtrage du trafic IPv6 »** (en plus du trafic IPv4) ;

- **laissez coché « Filtrage du trafic de bouclage »**, afin d'éviter les attaques de bouclage ;

- cochez « Bloquer le trafic d'IP fragmenté » car les paquets IP fragmentés peuvent être utilisés à des fins malveillantes ; **ne pas cocher** si vous utilisez des applications audio ou vidéo de haute qualité qui fragmentent les paquets IP, lors de l'utilisation de VPN, lors de certains jeux en ligne, ou si, par hasard, cela semble entraver une partie de votre trafic (cf. [2] « Gestion sécurisée du pare-feu » 1.6) ;

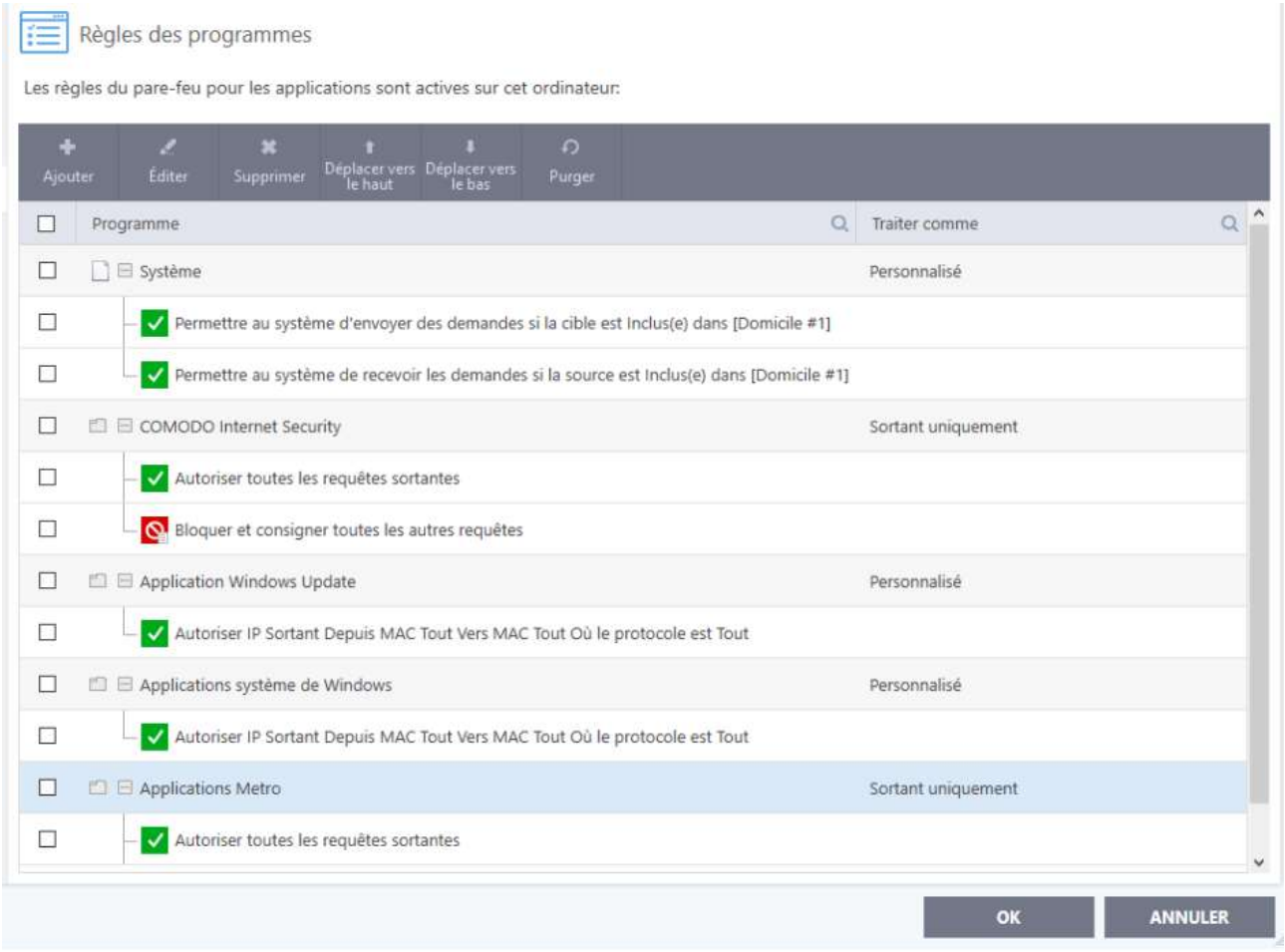
- **cochez « Analyser le protocole »** afin que les paquets non conformes aux protocoles standards soient bloqués par le pare-feu ;

- si vous avez un ordinateur isolé, ou un réseau local avec moins de trente objets connectés, **cochez « Activer l'anti-usurpation d'ARP »** afin d'éviter des attaques MITM (« Man in the Middle ») et DOS (« Denial of Service ») ; cf. [2] 1.4.3 ;

- ne pas oublier de valider le paramétrage en faisant OK en bas de chaque fenêtre.

10.2.2 Règles des programmes (vous n'avez rien à configurer pour l'instant)

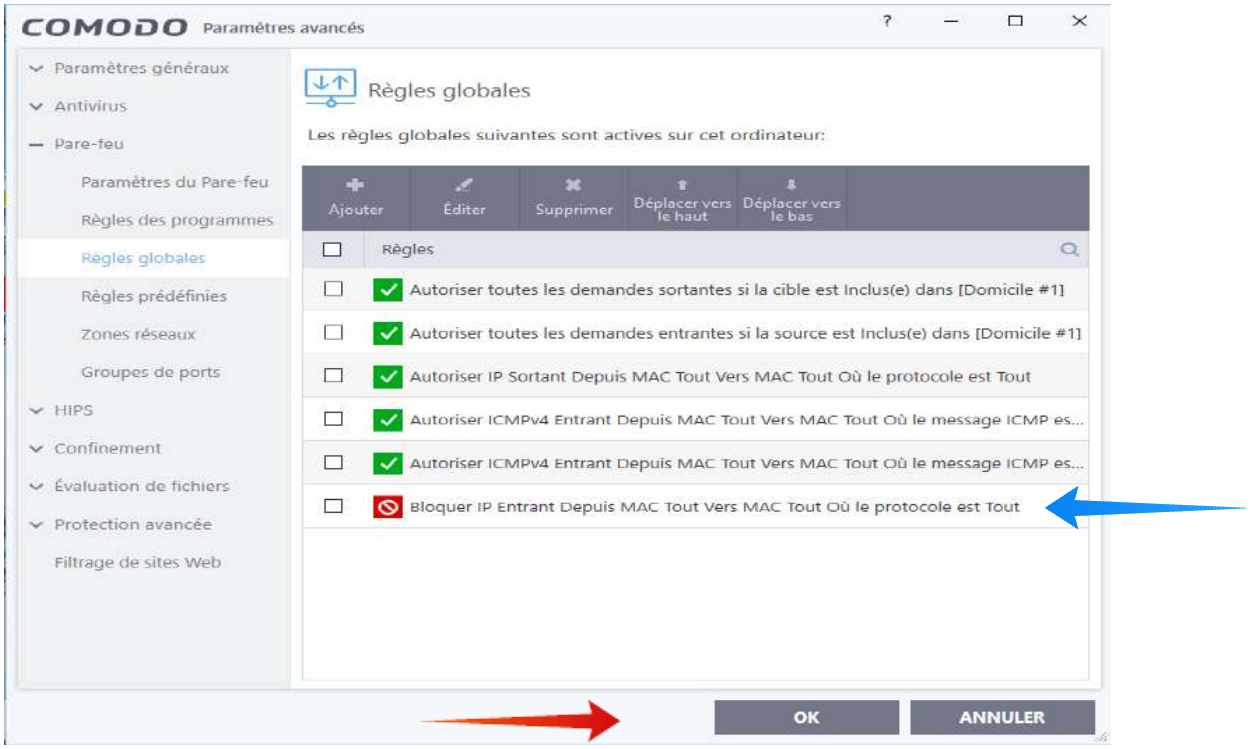
Voici, ci-dessous, juste après l'installation, les cinq premiers ensembles de règles :



Si vous avez coché en 10.2.1, c/ la case « Créer des règles ... », les règles de programmes se placeront, au fur et à mesure de leur création, au sommet de cette fenêtre où vous pourrez les consulter, les classer ou les modifier selon vos objectifs (cf. « [2] gestion sécurisée du pare-feu » 10.4).

10.2.3 Règles globales (vous n'avez rien à configurer pour l'instant)

L'option « Cacher les ports », activée en 9.2, *après que l'option « Je suis à mon domicile » ait été retenue en 5.4,* a engendré les six règles globales de la page suivante :



- les deux premières règles permettent à d'éventuelles règles de programmes, répondant aux mêmes spécifications, d'autoriser les connexions au réseau local (domicile # 1), l'une pour les demandes sortantes et l'autre pour les demandes entrantes ;

- la troisième règle permet à d'éventuelles règles de programme, répondant aux mêmes spécifications, d'autoriser les demandes de trafic IP sortant vers le réseau Internet ;

- les quatrième et cinquième règles globales autorisent deux messages différents en connexions entrantes, en provenance d'Internet, pour le protocole ICMPv4 ;

- la sixième règle bloque, pour l'ensemble des protocoles, toutes les demandes de connexions entrantes, à l'exception des demandes entrantes autorisées par les règles placées en lignes 2, 4 et 5, qui, du fait de leur position supérieure dans la fenêtre, sont prioritaires,

Des connexions entrantes supplémentaires ne doivent être autorisées que très exceptionnellement, lorsque cela est indispensable, par exemple pour une assistance à distance ou un jeu ; la règle devra alors être la plus restrictive possible avec mentions du protocole, si possible d'une adresse, et d'un ou quelques ports spécifiques, et être aussitôt transformée en règle de blocage dès la fin de cette pratique qui fragilise l'ordinateur (dans ce cas mieux vaut ne pas raccorder cet ordinateur au réseau local et ne pas l'utiliser pour des opérations bancaires ou sensibles),

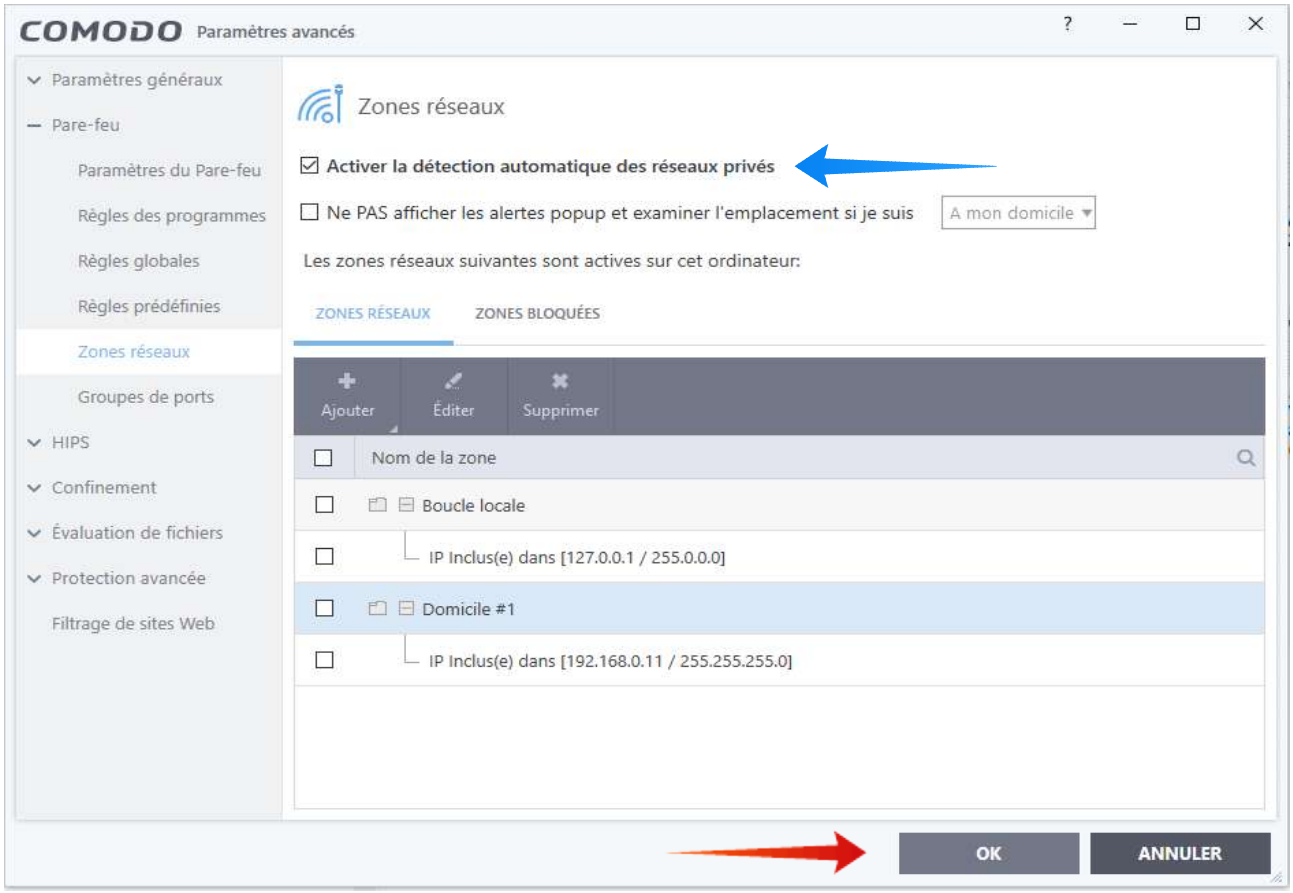
10.2.4 Règles prédéfinies

Comodo propose les règles prédéfinies suivantes :

- Navigateur internet ;
- Client de messagerie ;
- Client FTP ;
- Application autorisée ;
- Programme bloqué ;
- Sortant uniquement.

Nous verrons en *[2] 10.1* comment sécuriser deux de ces règles et en créer de nouvelles afin de limiter le nombre des alertes en mode **personnalisé** du pare-feu.

10.2.5 Zones réseaux



A moins que vous ne préfériez gérer vous-même les zones réseaux, laissez cochée la case « Activer la détection automatique des réseaux privés » :

10.2.6 Groupes de ports

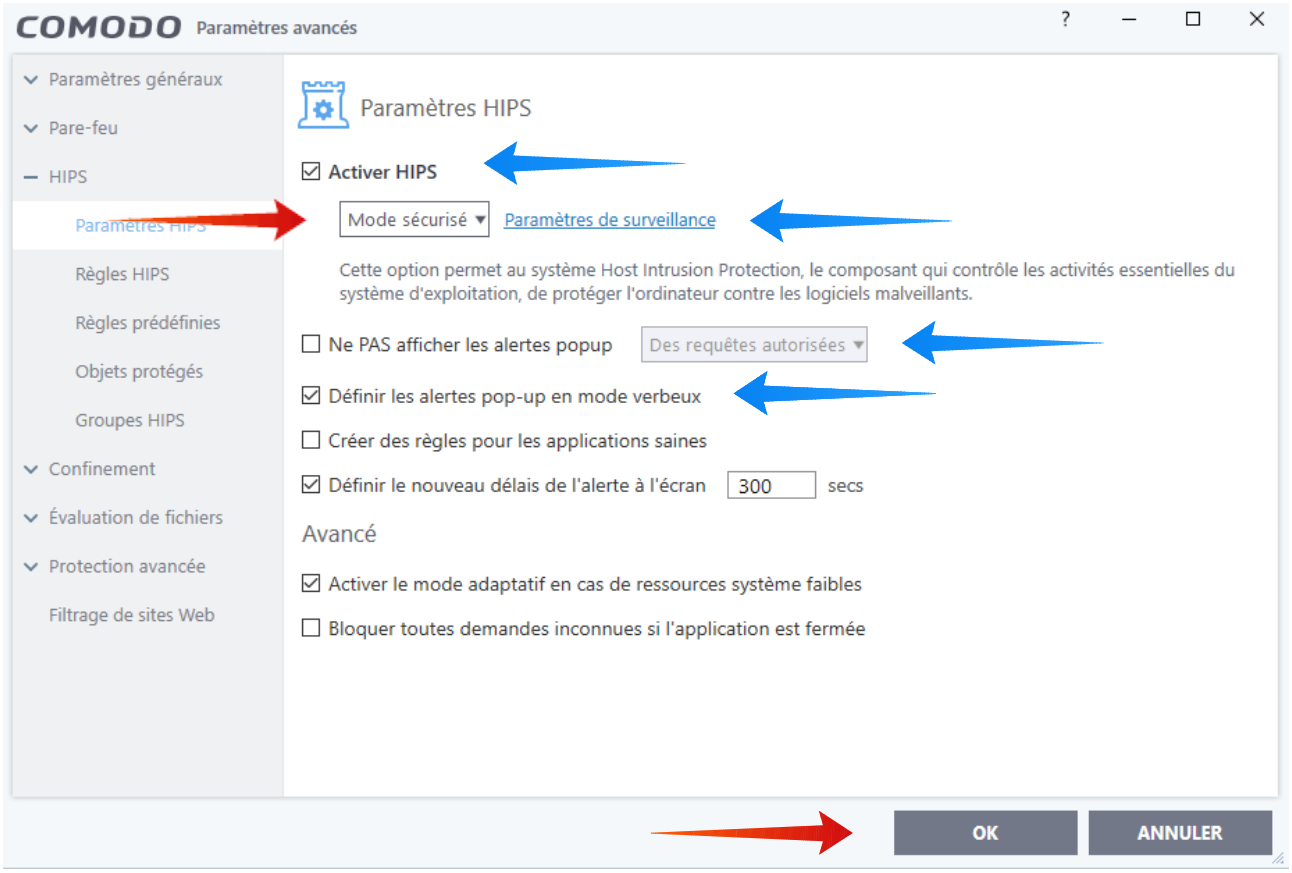
Vous pourrez ultérieurement utiliser les groupes de ports proposés par Comodo ou en créer de nouveaux selon vos besoins (cf. [2] 8,5)

10.3 HIPS

Nous verrons en [2] 1.4 que le module pare-feu gère principalement le trafic aux niveaux réseau (IP) et transport (TCP et UDP) des couches 3 et 4 du modèle TCP/IP ; cependant, lorsqu'une connexion est autorisée, il laisse passer tous les paquets d'informations liés à cette connexion, sans les analyser et sans s'assurer qu'ils sont sains.

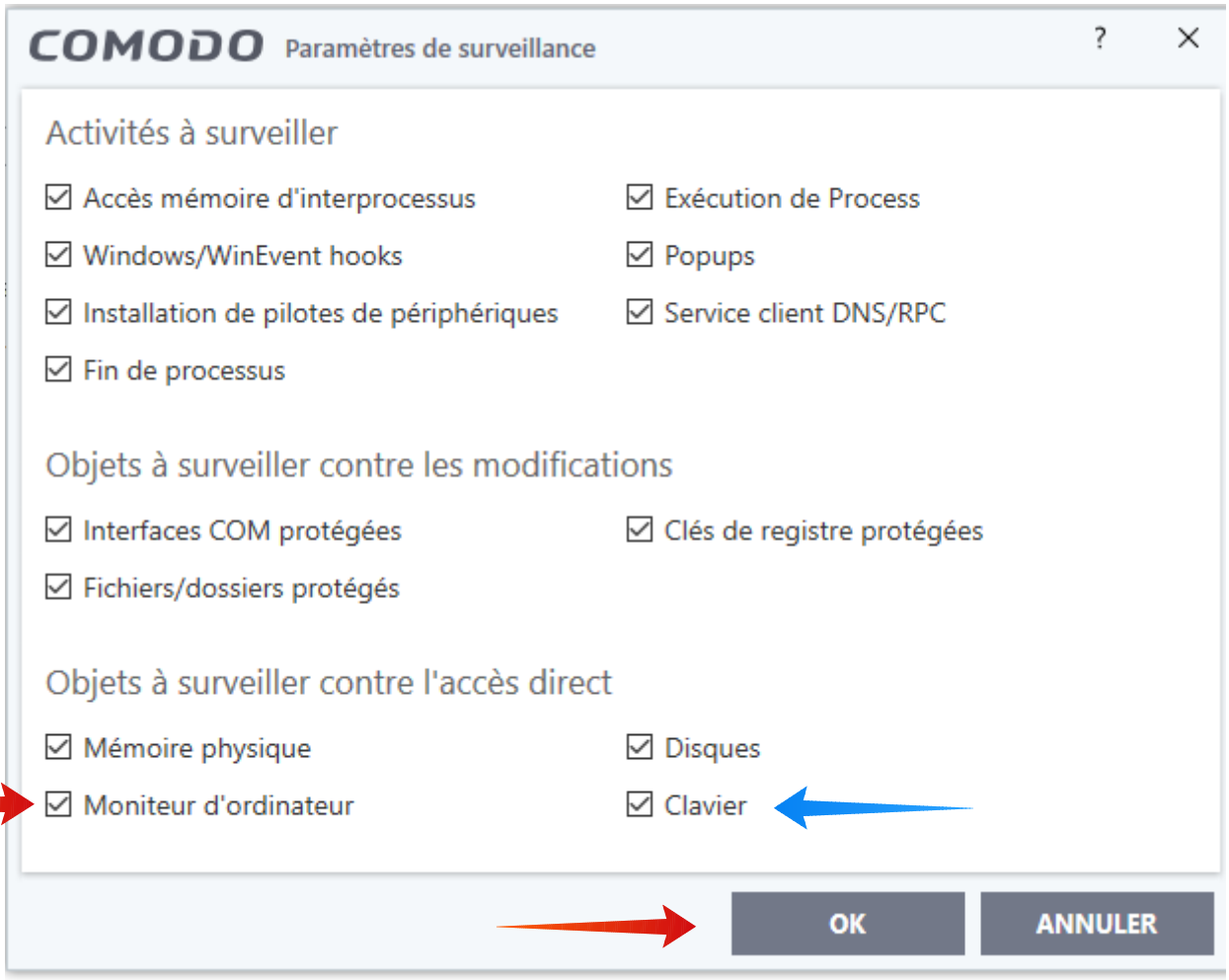
L'intérêt de Comodo Firewall provient de l'association, au module pare-feu proprement dit, du module HIPS qui complète ce dernier en surveillant les applications et les fichiers exécutables de l'ordinateur (couche « Applications » du modèle TCP/IP, située au dessus de la couche 4 de ce même modèle) et en empêchant ceux qui seraient malveillants de modifier les paramètres du système ;

10.3.1 Paramètres HIPS



a/ Choisissez le mode sécurisé ; cochez comme sur la fenêtre ci-dessus, et passez le délai d'alerte de 120 à 300 secondes.

b/ Avant de faire OK, cliquez, en haut à droite de la fenêtre, sur « Paramètres de surveillance » afin d'obtenir la fenêtre de la page suivante :



Cochez les deux dernières cases : toutes les cases doivent être cochées ;

- note : la surveillance du moniteur permet à Comodo de vous prévenir lorsqu'une application saine ou malveillante tente une capture d'écran ; et la surveillance du clavier de vous prévenir lorsqu'un « key logger » (enregistreur de touches) tente d'enregistrer les frappes du clavier à votre insu afin de s'emparer de vos mots de passe.

Ne pas oublier de valider le paramétrage en faisant OK en bas de cette fenêtre, puis, *ensuite,* de la fenêtre précédente.

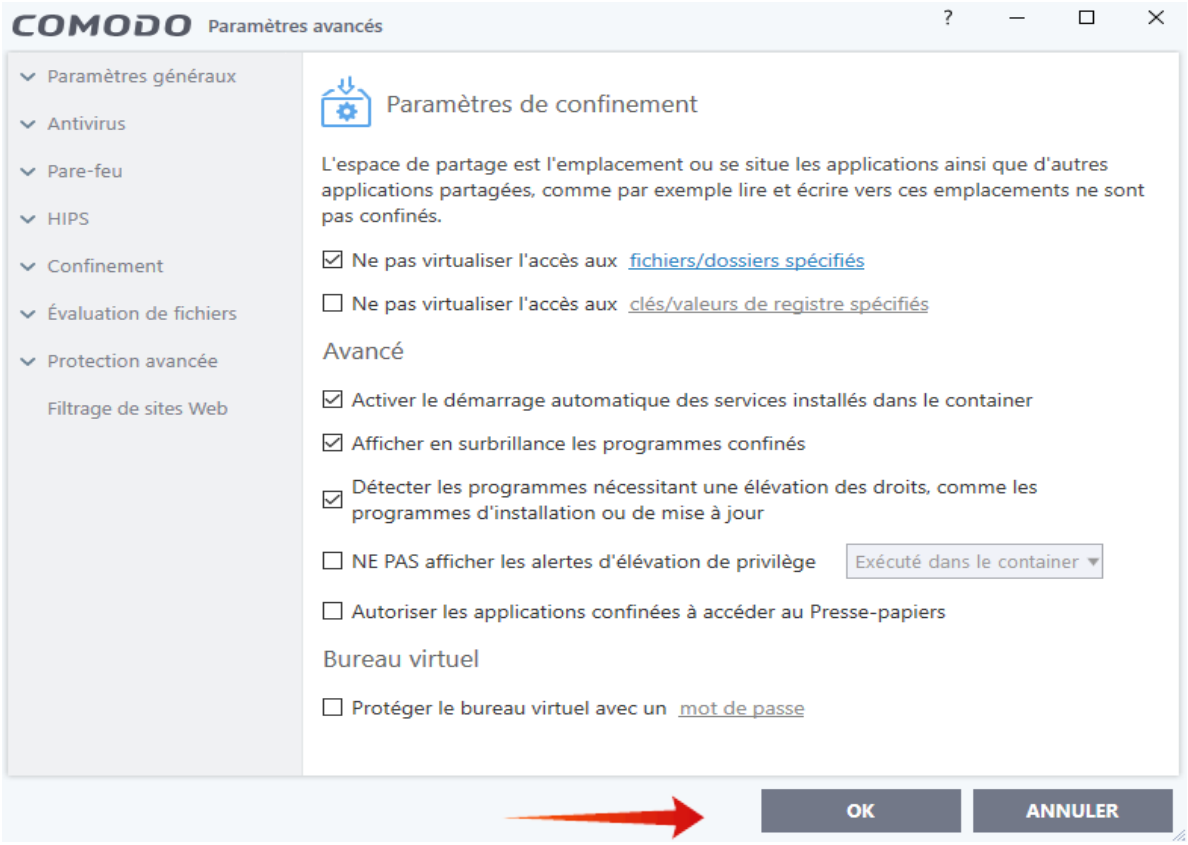
10.3.2 Règles HIPS : vous n'avez rien à paramétrer.

Comme nous avons choisi de ne pas cocher la case « Créer des règles pour les applications saines » en 10.3.1, cette fenêtre restera vide.

10.3.3 Règles prédéfinies (cf. [2] 10.1), **10.3.4 Objets protégés & 10.3.5 Groupes HIPS :** vous n'avez rien à paramétrer.

10.4 Confinement

10.4.1 Paramètres du confinement



Conservez les paramètres par défaut comme cochés ci-dessus ; cependant vous pouvez autoriser l'accès des applications confinées au presse-papier (redémarrage requis).

10.4.2 Confinement automatique

Conservez les paramètres par défaut, toutes les règles étant activées.

10.5 Evaluation de fichiers

10.5.1 Paramètres d'évaluation : *toutes les cases doivent rester cochées.*

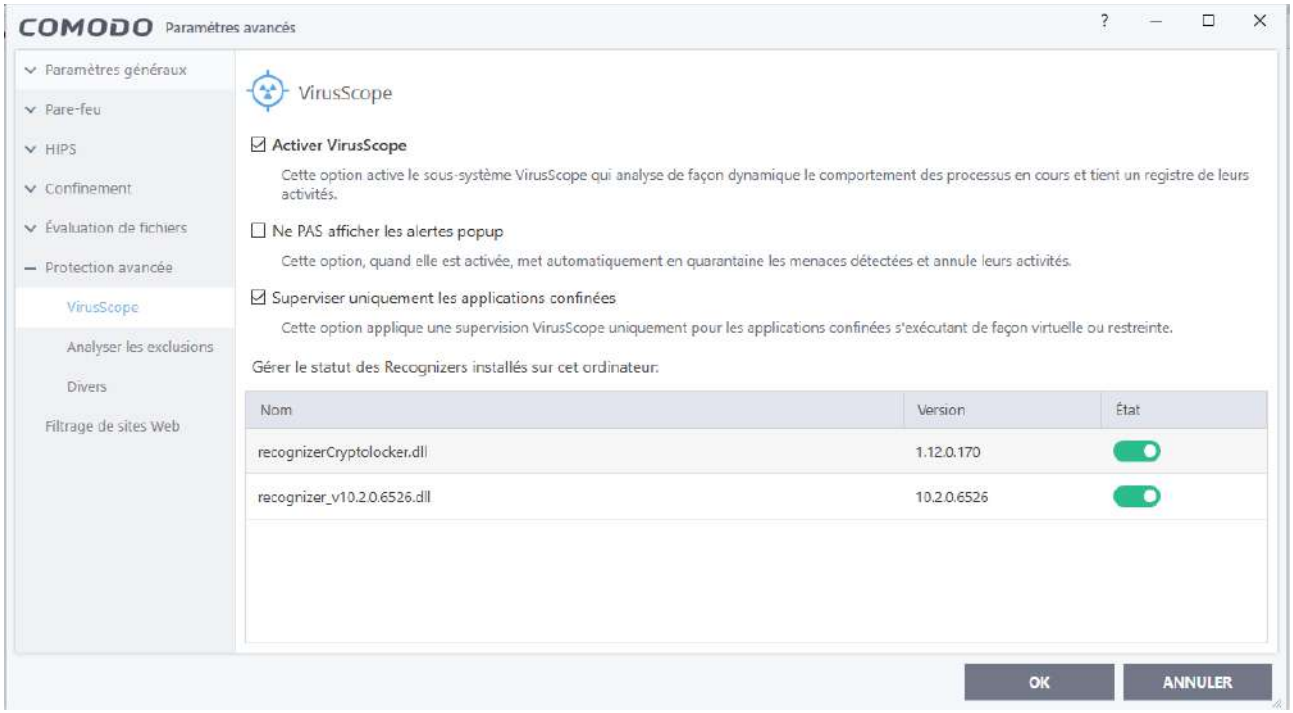
10.5.2 Groupes de fichiers : *vous n'avez rien à paramétrer,* mais il est instructif de

consulter les différents paragraphes de la fenêtre en cliquant sur les +.

10.5.3 à 10.5.5 : ***vous n'avez rien à configurer*** *sur les trois autres fenêtres de 10,5*

10.6 Protection avancée

10.6.1 Viruscope (rappelons que Viruscope n'est pas un antivirus)



Conservez les paramètres par défaut comme cochés ci-dessus ;

10.6.2 Analyser les exclusions, contrôle des périphériques, analyse des scripts

Vous n'avez rien à paramétrer.

10.6.3 Divers : ***vérifiez que les quatre cases sont cochées.***

10.6.4 Shopping Sécurisé : nous n'avons pas l'expérience de ce module

10.7 Filtrage de sites Web (cf. paragraphe 14) :

Sur la fenêtre de filtrage des sites Web, laissez cochée la case « Activer le filtrage des sites Web (recommandé) » , puis faîtes OK

11 Fin du paramétrage de la configuration de base du pare-feu de CIS

La configuration de base du pare-feu de CIC est désormais achevée. Il ne reste plus qu'à en assurer l'indispensable sécurisation (voir ci-dessous et paragraphe 12).

N'oubliez pas, dès à présent si vous avez installé le pare-feu isolé, ou après la configuration de l'antivirus si vous avez installé la suite complète, **de sauvegarder cette configuration en l'exportant dans un dossier de sauvegarde (cf.10.1.4)** : en cas de problème cela vous permettra de partir à nouveau de cette configuration, et d'éviter ainsi une reconfiguration complète ou même une ré-installation.

Pensez également à désactiver le pare-feu de Windows si vous ne l'avez déjà fait.

Avec cette configuration de base vous bénéficiez :
- de la protection de HIPS, de Viruscope et du module de filtrage des sites Web ;
- de la protection du container pour surfer sur Internet, pour ouvrir votre messagerie en toute sécurité ou pour essayer des programmes dont vous n'êtes pas sûr ;
- du fait que vos ports ont été cachés, et que pratiquement toutes les connexions entrantes en provenance d'Internet, à l'exception de deux règles pour ICMPv4, sont bloquées ;
- de la gestion dite sécurisée du pare-feu qui crée automatiquement des règles de programme pour les applications jugées saines par Comodo, et pour elles seules.

Il est essentiel que cette configuration de base soit sécurisée de façon simple (Niveau 1 de sécurisation) si vous ne désirez pas vous impliquer dans la gestion du pare-feu et que celle-ci soit assurée quasi automatiquement, ou de façon plus complexe si vous désirez contrôler personnellement la gestion du pare-feu de manière plus ou moins étroite (Niveaux 2 et 3 de sécurisation) : voir paragraphe 12 ci-dessous.

En cours d'utilisation vous avez intérêt :

a/ à désinstaller de votre ordinateur les programmes inutilisés ;

b/ à ne pas oublier de décocher la case « Se souvenir de ma réponse » lors de la réponse à une alerte déclenchée par une règle « Demander », sinon une nouvelle règle « Autoriser » ou « Bloquer » sera créée et se substituera à la règle « Demander ».

c/ à suivre périodiquement, dans la fenêtre des « Règles de programmes », la création des nouvelles règles, afin de les modifier si nécessaire ;

12 Sécurisation de la configuration de base du pare-feu

Les configurations par défaut du module pare-feu de Comodo, ainsi que des pare-feux Windows et de diverses suites, ne sont pas optimales car ces pare-feux doivent pouvoir être employés par des utilisateurs ayant des profils très différents : simples particuliers utilisant essentiellement le Web, la messagerie et quelques applications de base (traitement de texte, photo, généalogie …), joueurs, professionnels divers, petites et grandes entreprises, etc …

Le pare-feu Comodo étant suffisamment souple, la gestion du trafic peut être traitée de diverses façons selon que vous souhaitez ne plus avoir à intervenir lors de son fonctionnement ou, au contraire, que vous souhaitez contrôler de manière plus ou moins étroite, c'est -à-dire plus ou moins sécurisée, le trafic entre votre ordinateur et les réseaux Internet et local. Nous présentons ici, et développons dans le second tutoriel [2], ***trois niveaux de sécurité croissante du pare-feu, les niveaux 2 et 3 supposant que le précédent niveau ait été mis en place.***

- **le Niveau 1 de sécurité** (cf. [2] 9) assure aux utilisateurs qui ne désirent pas s'impliquer dans la gestion du pare-feu et aux nouveaux utilisateurs qui ne sont pas encore familiarisés avec le pare-feu une relative, mais bien meilleure sécurité que le pare-feu Windows : il nécessite une demi-heure environ de paramétrage initial, après quoi la gestion du pare-feu **en mode sécurisé** sera quasiment automatique, pour les demandes de connexions de toutes les applications jugées saines par Comodo, et avec seulement de rares alertes pour les demandes des autres applications.

- **le Niveau 2 de sécurité** (cf. [2] 10) assure un niveau accru de sécurité ; il utilise **le mode personnalisé** de gestion du pare-feu dans lequel ce dernier traite lui-même les demandes de connexions des applications selon les règles déjà spécifiées par l'utilisateur ; en l'absence de règle déjà spécifiée le pare-feu envoie une alerte à l'utilisateur qui, éclairé par le conseil et les informations fournies par l'alerte, n'autorisera que les demandes des seules applications qui lui sont nécessaires ; il nécessite un certain travail de l'utilisateur pour le paramétrage initial ; les alertes du pare-feu seront nombreuses lors des premiers jours, puis deviendront ensuite peu fréquentes car les principales règles de programmes auront été créées ;

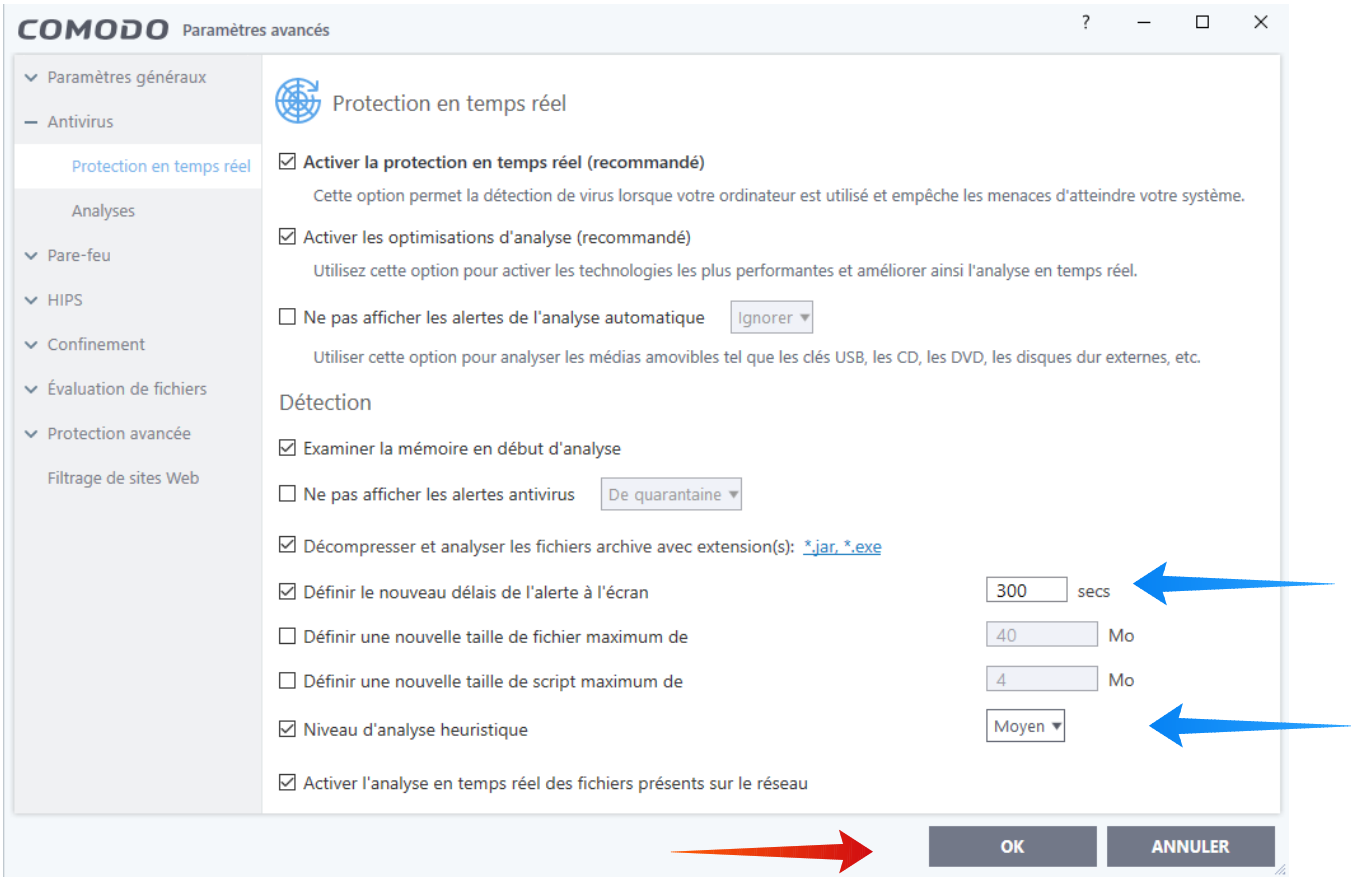
- **le Niveau 3 de sécurité** (cf. [2] 11) est destiné aux utilisateurs davantage expérimentés, ayant déjà utilisé le Niveau 2 et qui désirent exercer **un contrôle étroit du trafic** ; il permet à l'utilisateur de contrôler toutes les connexions entrantes et sortantes de son ordinateur avec Internet et son réseau local (imprimante, télévision et

autres objets connectés).

13 Configuration de l'antivirus (pour la suite seulement)

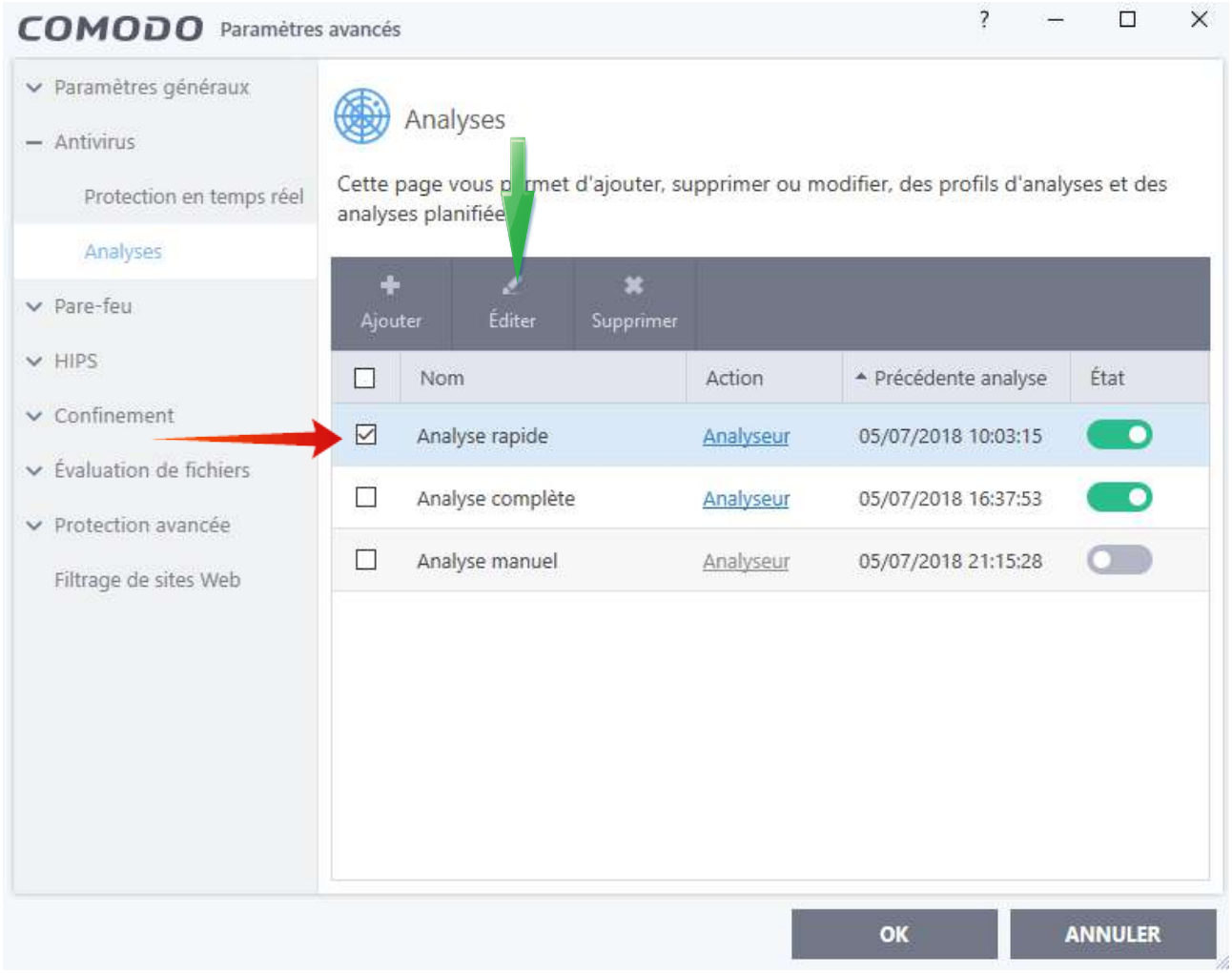
13.1 Protection en temps réel

Vous pouvez configurer comme ci-dessous, puis faire « OK » :



Toutefois si l'ordinateur se trouvait ralenti, vous pourriez abaisser le niveau d'analyse heuristique à « Bas »

13.2 Analyses



- afin de paramétrer un type d'analyse : cocher la case correspondante, puis **double** cliquer sur éditer pour ouvrir la fenêtre de paramétrage correspondante ; cliquer sur OK, seulement après le paramétrage des différents types d'analyse.

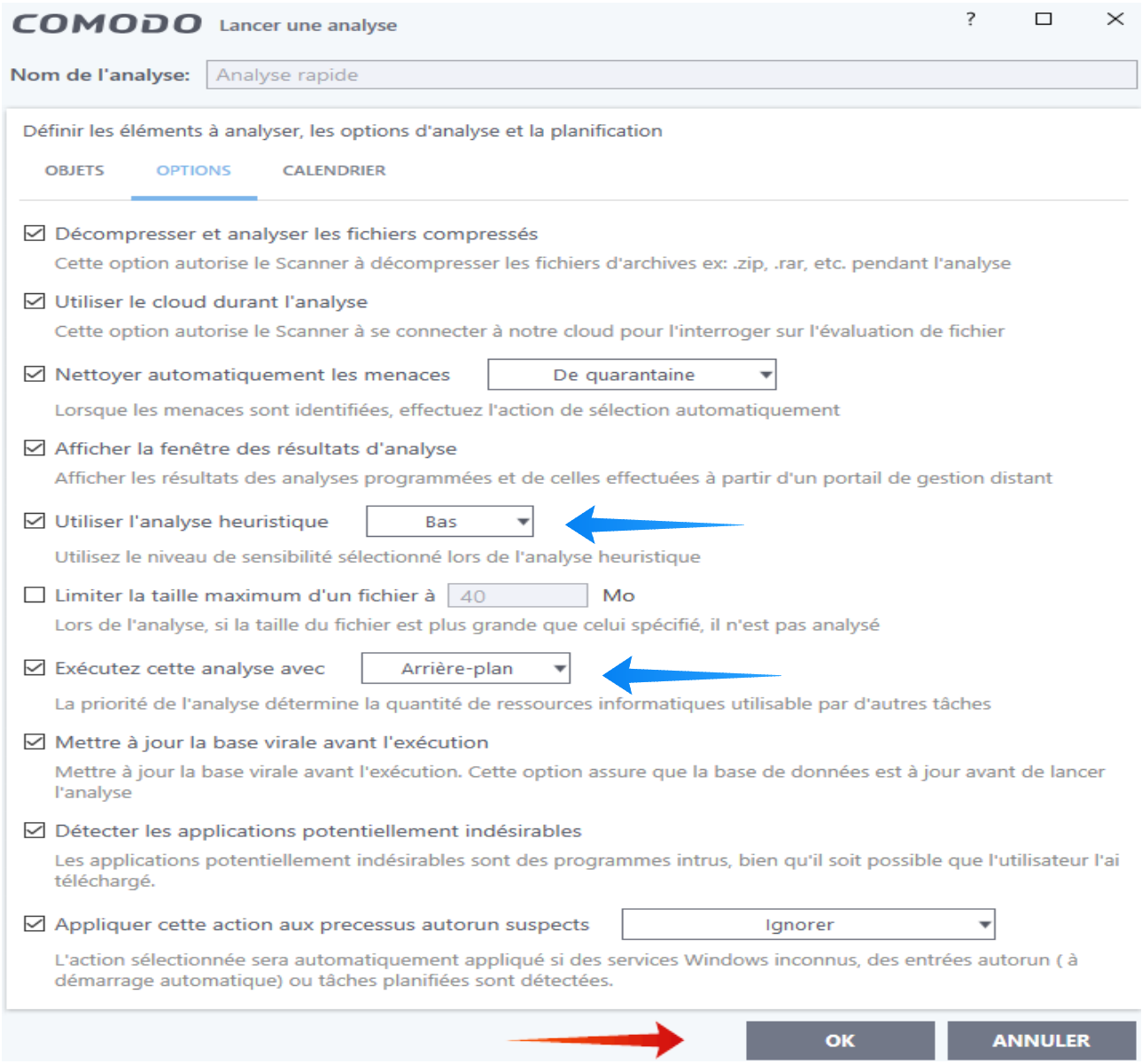
13.2.1 Analyse rapide

a/ Sous l'onglet « Objets »

- Garder le réglage par défaut **« Les secteurs souvent infectés »**.

- Vous pouvez ajouter des fichiers, un répertoire, une région, mais l'analyse sera moins rapide.

b/ sous l'onglet « Options » vous pouvez paramétrer comme ci-dessous :



Il faut lire :

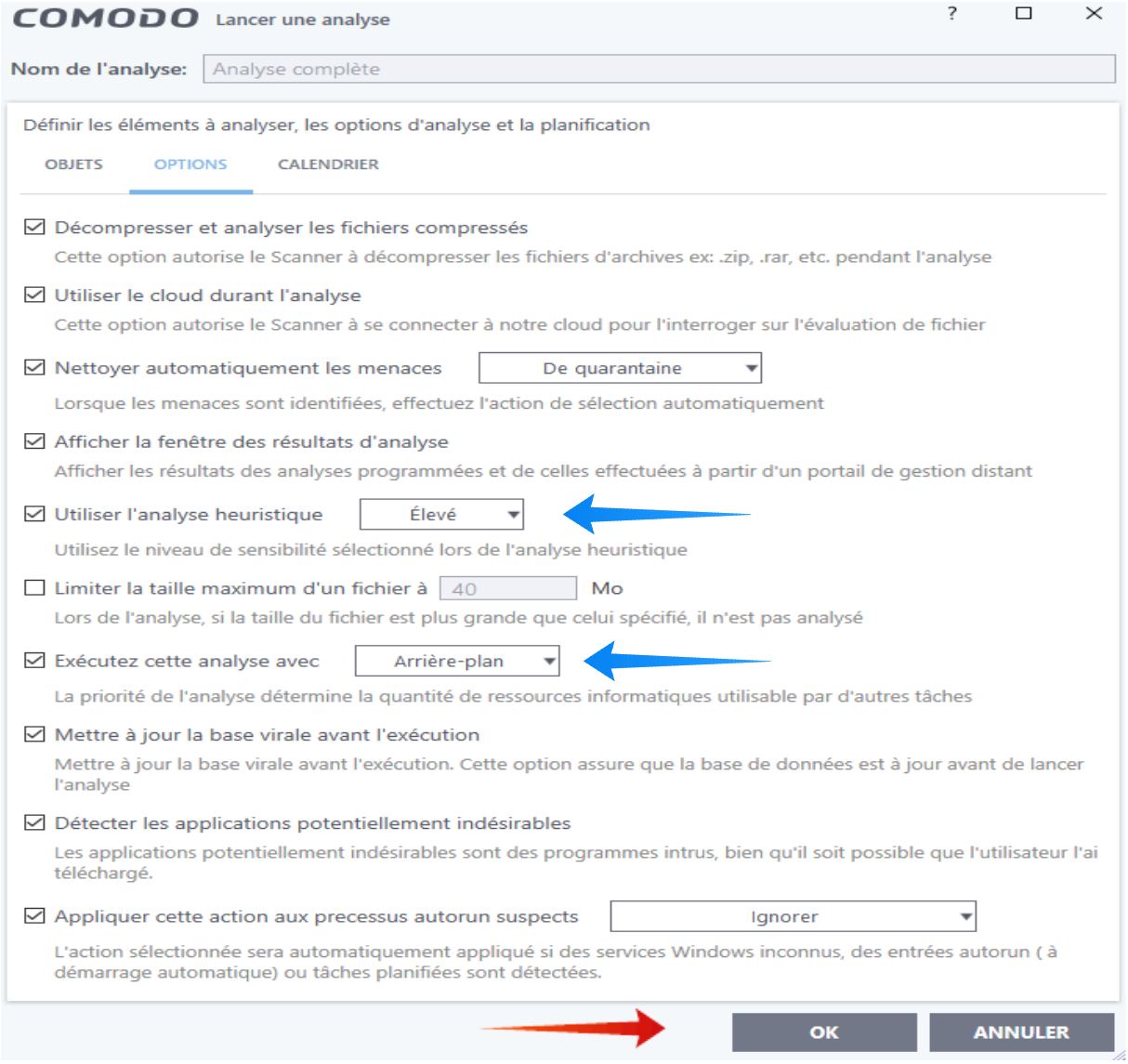
- Nettoyer automatiquement les menaces avec mise en quarantaine (pour « de quarantaine »);

- Exécutez cette analyse en arrière-plan (pour « avec arrière-plan »).

Ne pas oublier de faire OK pour chaque fenêtre.

c/ sous l'onglet « Calendrier », dans la fenêtre qui s'ouvre, on pourra choisir par exemple : heure de début 10 h, chaque jour, exécuter uniquement lorsque l'ordinateur n'est pas sur batterie ; faire OK avant de quitter.

13.2.2 Analyse complète : paramétrer comme ci-dessous



- « **Utiliser l'analyse heuristique » : de niveau élevé,** pour l'analyse complète
- **« Exécuter cette analyse »** (choix de priorité) : Haut, Normal, Bas, En arrière-plan ; retenez « En arrière-plan » si vous travaillez ou « Haut » dans le cas contraire ;

- Objets : cochez « Tout l'ordinateur », et « La mémoire » ;

- Calendrier : l'analyse pourra, par exemple, être programmée chaque semaine.

13.2.3 Analyse manuelle

13.2.4 Vous pouvez ajouter autant de profils d'analyse que vous le désirez.

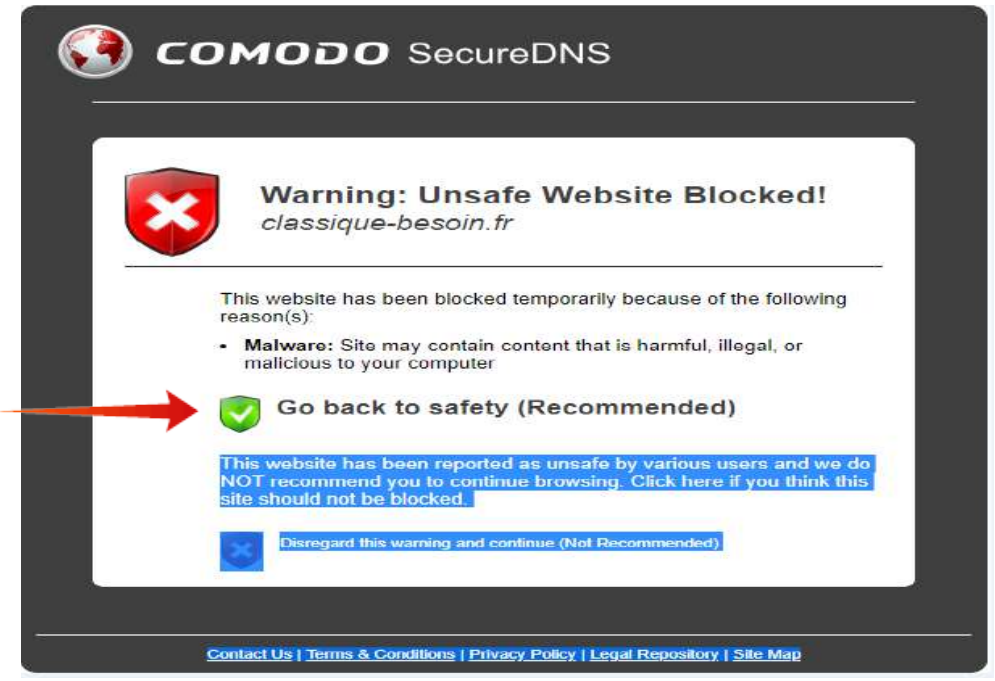
Partie 3 - Navigateurs sécurisés et conteneur

14 Dragon et IceDragon, les navigateurs sécurisés de Comodo

Les navigateurs de Comodo, que ce soit IceDragon, version sécurisée de Firefox, ou Dragon, version sécurisée de Chrome, jouent un rôle essentiel dans la protection de votre navigation sur le Web, ils bénéficient en effet :

- **de la fonction de recherche de liens de SiteInspector**, permettant de vérifier si une page Web est malveillante ou non ;

- **de la réduction des risques d'empoisonnement du cache DNS et de la fonction de filtrage des sites malveillants par les serveurs SecureDNS de Comodo** : cf. l'alerte ci-dessous, l'une des rares qui n'ait pas été traduite en français :



- **de la protection du conteneur, lorsque les navigateurs y ont été placés** : ainsi, même en cas de contamination par un malfaisant, celui-ci ne peut se propager à votre ordinateur et reste cantonné au conteneur.

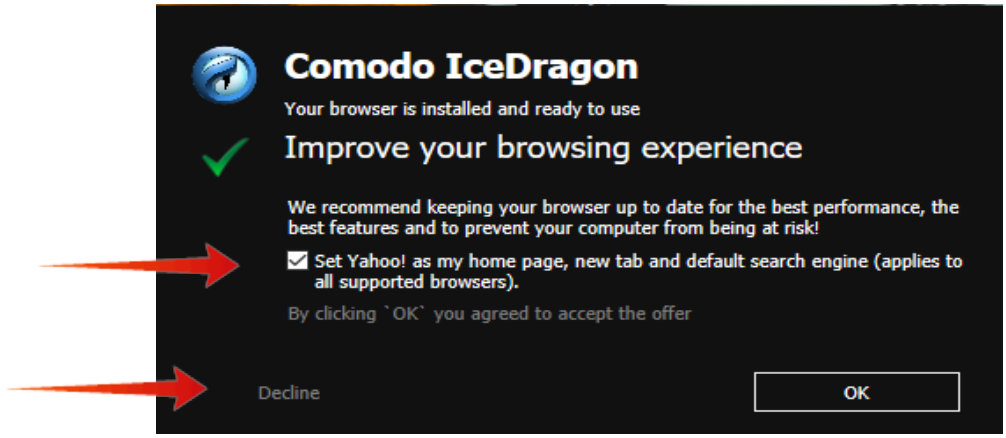
Les appellations d'IceDragon et de Dragon recouvrent en fait les navigateurs Firefox et Chrome avec les mêmes moteurs et configurations, mais davantage sécurisés ; vous pourrez donc. conserver les mêmes réglages et importer vos favoris sans problème. Vous trouverez les manuels d'utilisation en anglais en [11] et en [12] et vous pouvez également utiliser les tutoriels de Firefox et de Chrome publiés en français.

14.1 Installation de Dragon

L'installation se fait en même temps que celle de la suite ou du pare-feu si la case adéquate a été cochée au cours de celle-ci ; il est alors possible de lancer Dragon de l'intérieur du conteneur.
Elle peut également être faite de manière indépendante, après téléchargement, grâce au lien ci-après : https://www.comodo.com/home/browsers-toolbars/browser.php

14.2 Installation d'IceDragon à partir du lien : https://icedragon.comodo.com/

- après une première fenêtre d'agrément de la licence, vous rencontrerez :
- la deuxième fenêtre qui vous propose le lieu d'installation d'IceDragon ;
- la troisième fenêtre où vous suivrez la progression du processus d'installation ;
- la quatrième fenêtre où vous pourrez lancer IceDragon et le choisir ou non comme navigateur par défaut ;
- après le lancement si vous ne désirez pas Yahoo comme page d'accueil (home page) vous décocherez la case « Set Yahoo » et cliquerez sur « Decline » comme ci-dessous

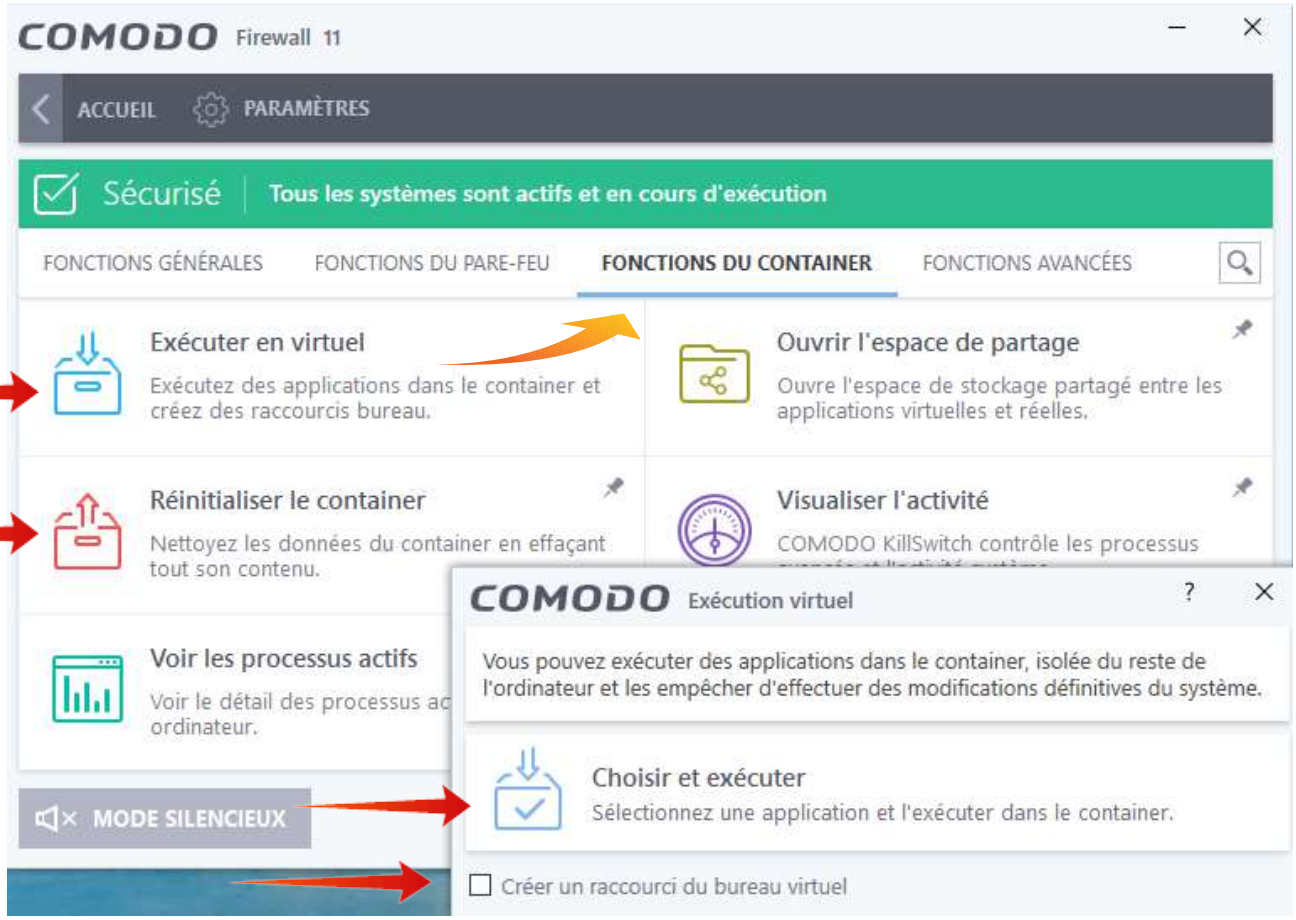


- IceDragon est désormais utilisable sur votre ordinateur, mais si vous voulez naviguer sur le Web en étant protégé des malfaisants, il est nécessaire de préparer son utilisation dans le conteneur comme ci-dessous.

15 Utilisation du conteneur

15.1 Utilisation d'un programme dans le conteneur (exemple avec IceDragon)

A partir de la fenêtre principale cliquez sur l'onglet Fonctions, puis dans la nouvelle fenêtre, sur l'onglet « Fonctions du conteneur » ;



- cliquez dans l'ordre sur :

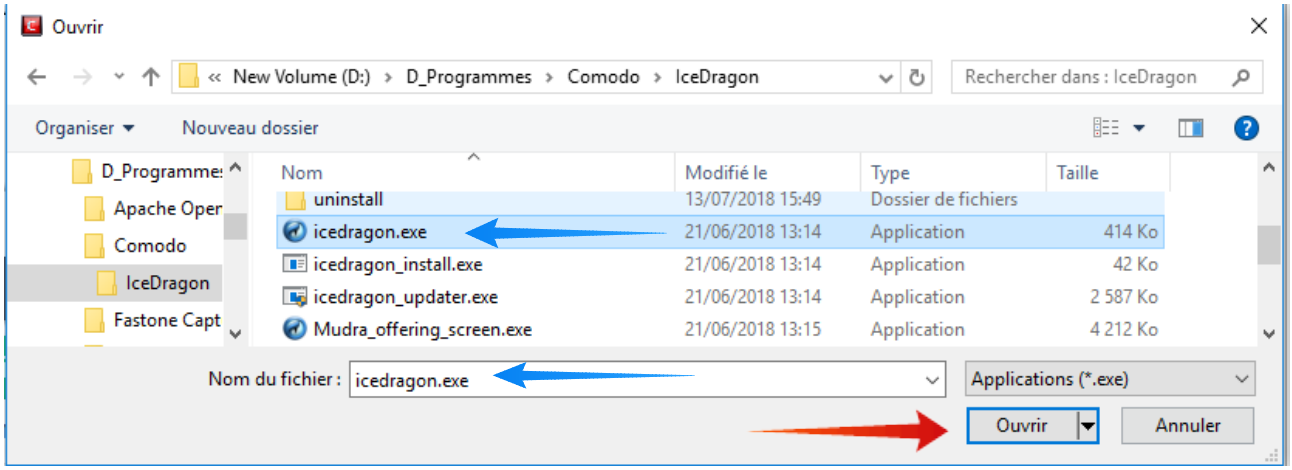
a/ « Exécuter en virtuel », une nouvelle fenêtre s'ouvre ;

b/ dans cette nouvelle fenêtre, cochez la case « Créer un raccourci du bureau

virtuel » ;

c/ puis cliquez sur « Choisir et exécuter » ;

d/ **rendez-vous alors sur le lieu d'installation du programme :** *ci-dessous avec l'exemple d'IceDragon,* ici sur le disque D, mais plus classiquement sur Windows (C)\Programmes\Comodo\Ice-Dragon ou ProgramFiles (x86)\Comodo\Ice-Dragon.



- **sélectionnez alors « icedragon.exe »** pour le faire apparaître dans « Nom du fichier » ;

- **puis cliquez sur « Ouvrir » :** *Ice-Dragon est désormais utilisable dans le conteneur et un raccourci « IceDragon Virtuel » est désormais sur le bureau ; pour un accès plus aisé vous pouvez le glisser dans la barre des tâches :*

15.2 Autres navigateurs placés dans le container

On peut aussi placer Firefox et Edge dans le conteneur, ils bénéficieront de sa protection, mais pas, comme pour Dragon et IceDragon, de la sécurisation par SiteInspector et SecureDNS.

15.3 Limitations pour les navigateurs placés dans le container

La contrepartie de la protection assurée par le container est que :
- l'on ne peut déposer de copier-coller en provenance de la zone hors du container dans la barre d'adresses d'un navigateur qui s'y trouve placé ;
- l'on ne peut installer un programme hors container à partir d'un téléchargement effectué dans le container : il est alors nécessaire d'effectuer le téléchargement avec le navigateur hors du container (un navigateur utilisé dans le container demeure disponible hors container).

15.4 Réinitialiser le conteneur

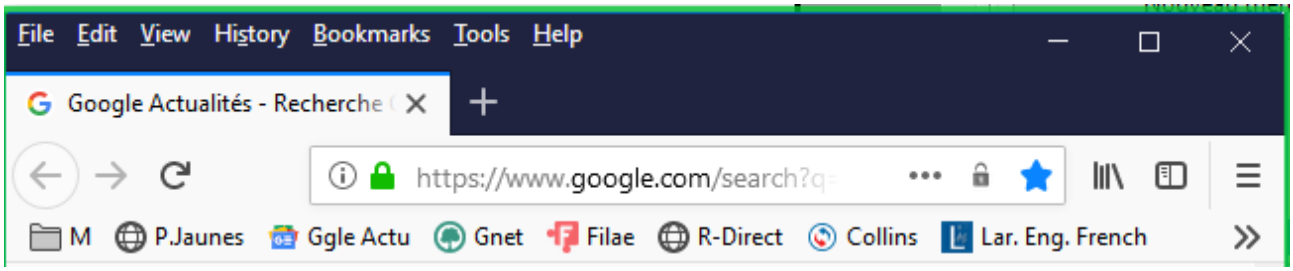
Pensez à réinitialiser le conteneur de temps à autre en cliquant sur la deuxième option de la fenêtre de « Fonctions du conteneur », vous le nettoierez ainsi des éventuelles données contaminées ; cette option peut également être employée lorsque l'accès à un programme situé dans le container devient impossible.

16 Aménagement d'IceDragon

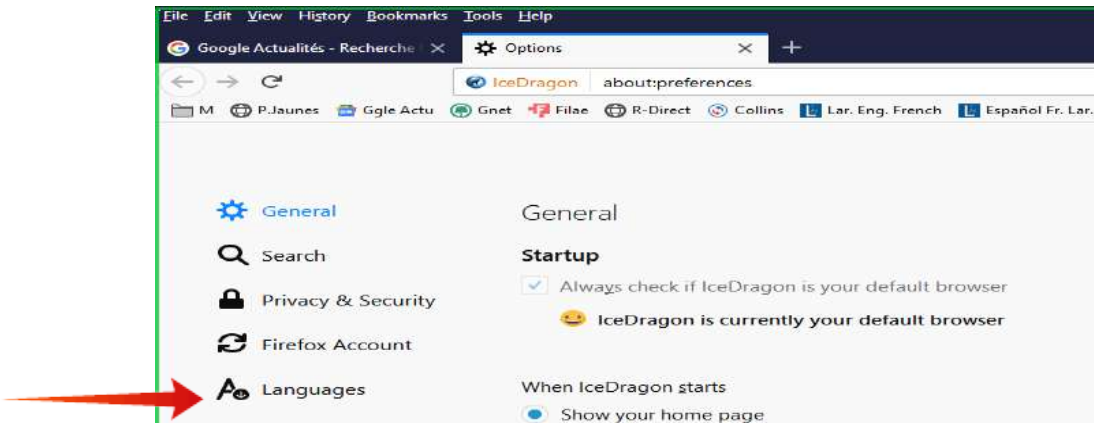
Un fois installé, IceDragon est quasiment identique à Firefox, aussi ne signalerons-nous que quelques points de configuration ; à la première ouverture vous obtenez ceci dans la partie supérieure de la fenêtre :

- le cadre vert entourant la fenêtre signale qu'IceDragon est dans le conteneur, vous pouvez désormais naviguer sur le Web en étant protégé ;

- un clic droit sur la partie noire ouvre un menu déroulant qui vous permet de sélectionner : la barre de menu (Menu Bar), la Barre de favoris (Bookmarks Toolbar) et d'ouvrir le menu « Personnalisez » (Customize) ; la sélection des barres donne :

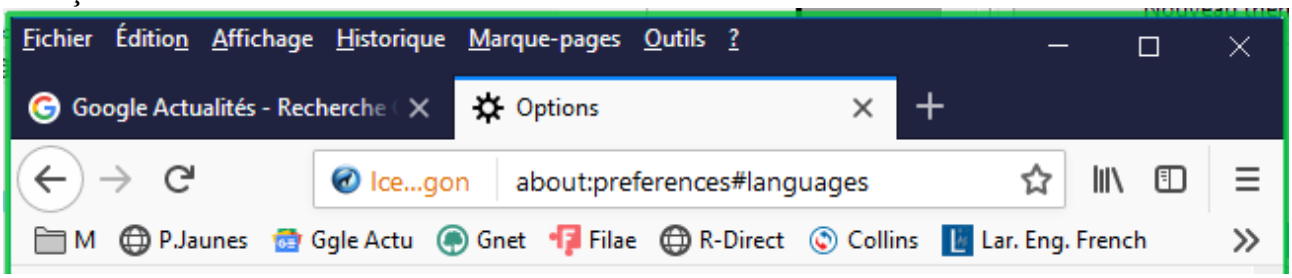


- un clic sur Tools (Outils), puis, dans le menu déroulant, sur Options conduit à :

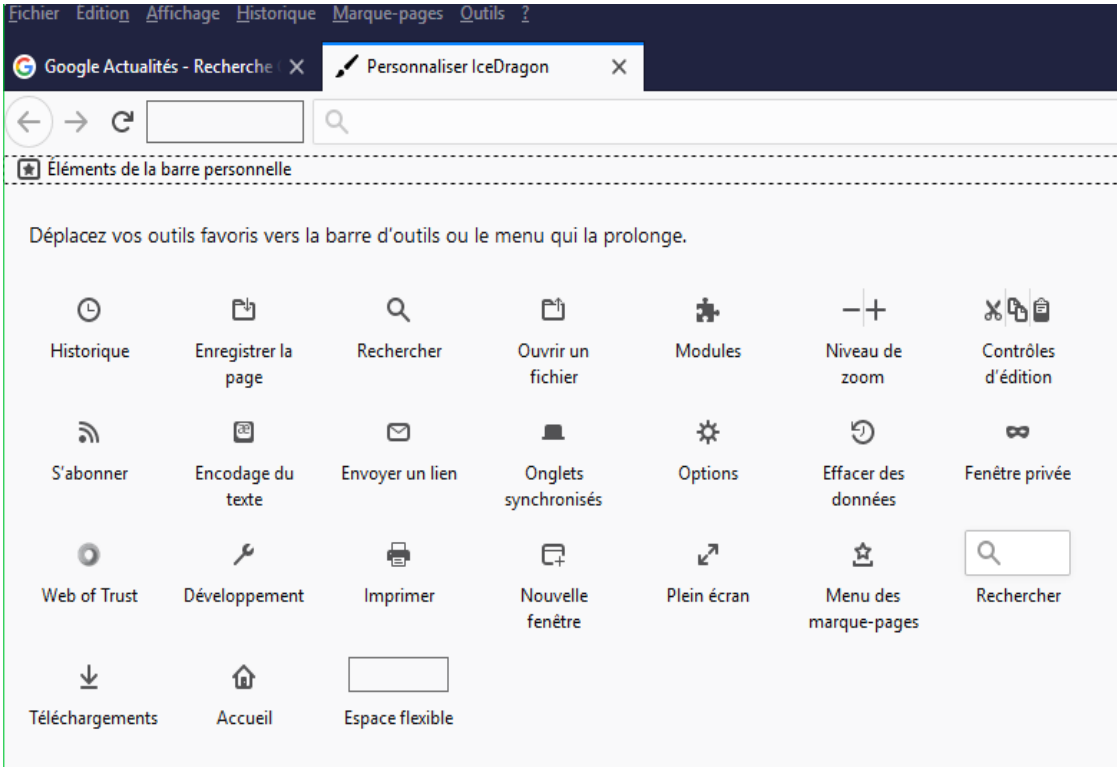


- en cliquant sur Languages, vous ouvrez la fenêtre où vous pourrez sélectionner le

français :



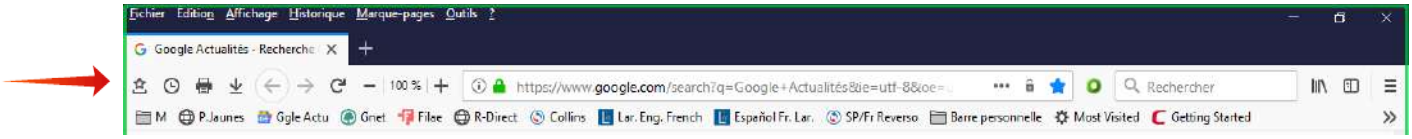
- en cliquant sur « Marque-pages » puis en sélectionnant « Afficher tous les marque-pages » vous accédez à la fenêtre de gestion des marque-pages et de la barre personnelle, où vous pourrez choisir « Importation et sauvegarde » des marque-pages au format HTML (par exemple d'importer vos marque-pages de Firefox ou d'un autre navigateur, ou de déplacer et classer ces marque-pages) ;



- après un nouveau clic dans la partie noire, choisir « Personnaliser » ; vous atteignez alors le menu ci-dessus, d'où nous allons glisser les icônes de notre choix vers la barre personnelle : ici « Menu des marque-pages », « Historique », «Imprimer », « Téléchargements », « Niveau de Zoom », et l'espace « Rechercher » ;

Les icônes déplacées sont désormais dans la barre personnelle : à partir de celle-ci

vous pouvez afficher les menus correspondants ou déclencher les actions voulues :



Partie 4 - Migration de la suite au pare-feu ; désinstallation du produit

17 Désinstallation partielle (migration) ou totale de la suite ou du pare-feu

Afin d'éviter toute difficulté Comodo recommande de ne pas interrompre une désinstallation ou une installation en cours.

Dès la fin de l'installation il est possible de désinstaller l'un des modules, antivirus ou pare-feu, pour ne garder que l'autre. Le module désinstallé pourra ensuite être réinstallé à tout moment. *Ainsi peut-on télécharger la suite pour n'utiliser que le pare-feu ou l'antivirus.*

17.1 Tronc commun à la réparation, à la migration et à la désinstallation

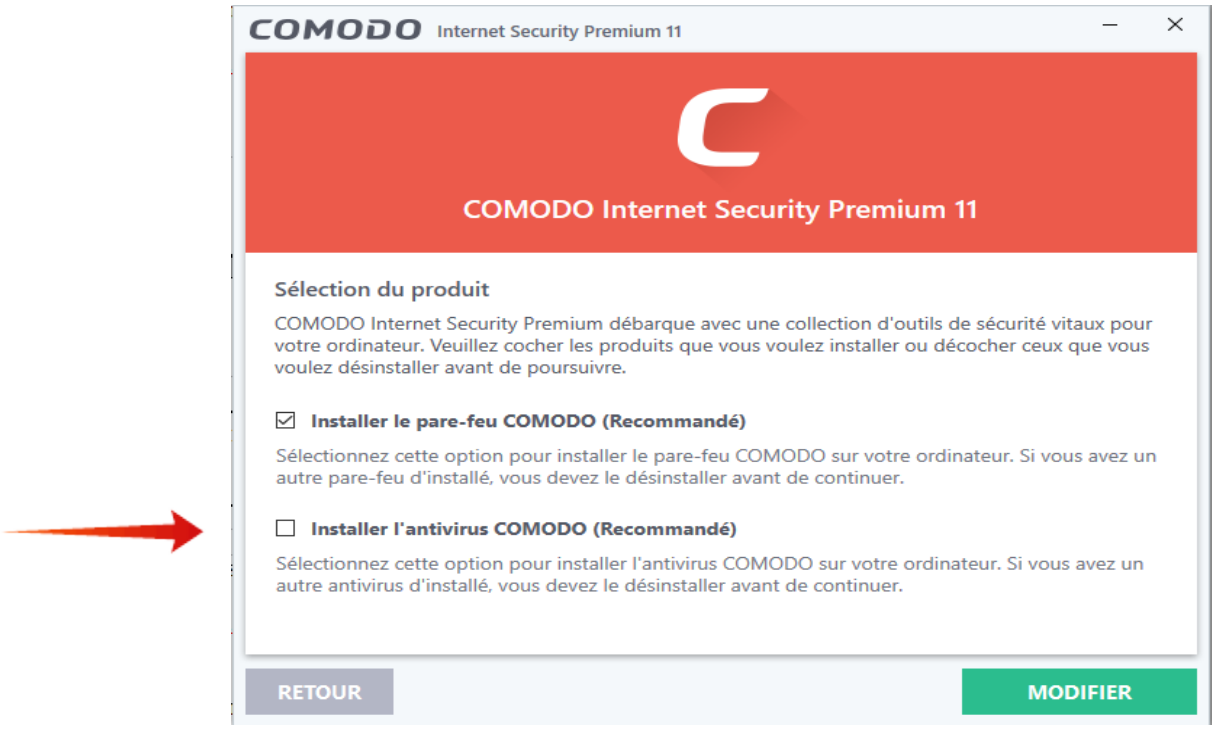
A partir du menu « Programmes et fonctionnalités » du panneau de configuration, faîtes un clic droit sur « Comodo Internet Security Premium » : vous obtenez « Désintaller/Modifier », cliquez à nouveau, vous obtiendrez la fenêtre ci-dessous :

A partir de la fenêtre de la page précédente vous pouvez réparer la suite, la

modifier pour ne garder qu'une des deux fonctionnalités ou la désinstaller totalement :

17.2 Migration de la suite au pare-feu et vice-versa

Un clic sur « Modifier », dans la fenêtre précédente, vous conduit à la fenêtre ci-dessous :



Décochez « Installer l'antivirus Comodo » pour ne garder que le pare-feu (ou vice-versa), puis cliquez sur « Modifier » (en vert) ; la désinstallation partielle démarre et vous demande un redémarrage qui peut durer de 2 à 10 minutes.

Il sera ultérieurement possible de réinstaller la fonction désinstallée en utilisant le même processus.

17.3 « Désinstaller » vous conduit à une fenêtre qui vous demande si vous

désirez :

a/ réinstaller ultérieurement le produit ou le remplacer par une autre version : certains éléments du programme seront alors conservés ;

b/ ou retirer définitivement le produit : la désinstallation sera alors approfondie

Avant de débuter la désinstallation :

- faire un point de restauration ;
- réactiver le pare-feu Windows en bloquant toutes les connexions entrantes ;
- désactiver tous les modules de la suite, puis cliquer sur l'option choisie ;

A la fin de la désinstallation, Comodo vous demande de redémarrer

Note : les antivirus et pare-feux sont le plus souvent protégés de leur désinstallation par des programmes malfaisants, ce qui peut, parfois, rendre une désinstallation totale légitime difficile.

En cas de problème éventuel, vous pouvez, comme pour les autres antivirus, compléter la désinstallation par un nettoyage des fichiers et du registre par C-Cleaner sur les différents comptes utilisateurs (et administrateur) et la compléter par une éradication manuelle, en tant qu'administrateur, dans le dossier Windows (C:), d'éventuels résidus, si nécessaire en mode sans échec, au niveau de Program Files, Program Data, Programmes, et, pour chacun des utilisateurs, au niveau des sous-dossiers Local, LocalLow et Roaming de leur dossier AppData ; mais, selon notre propre expérience, cela n'est pas nécessaire car, après le nettoyage avec C-Cleaner correctement paramétré, il ne reste plus de fichiers Comodo.

17.4 Outil spécial de désinstallation de Comodo [14]

La désinstallation du programme doit en priorité être effectuée selon la méthode traditionnelle décrite ci-dessus.

Ce n'est qu'en cas de difficulté avec cette méthode traditionnelle que Comodo propose, depuis décembre 2017, d'utiliser un outil de désinstallation en y joignant un avertissement qui vous informe **que vous assumez tous les risques de perte ou de dommage en utilisant cet outil et que Comodo ne pourra être tenu pour responsable de toute perte ou dommage** (cet avertissement nous rend

personnellement circonspect sur l'utilisation de cet outil que nous n'avons jamais employé).

Voici ci-dessous le mode d'emploi de cet outil obligeamment traduit par Zorkas que nous remercions vivement ;

« L'outil de désinstallation de Comodo permet aux administrateurs et aux utilisateurs avancés d'analyser les hôtes pour les produits Comodo et de les supprimer. Les produits pouvant être supprimés par cet outil sont Comodo Internet Security, Comodo Firewall et Comodo antivirus.

a/ Téléchargez l'un des deux fichiers d'installation ci-dessous :

- Version 64 bits :
https://download.comodo.com/cis/download/installs/ciscleanuptool/ciscleanuptool_x64.exe

-Version 32 bits :
:https://download.comodo.com/cis/download/installs/ciscleanuptool/ciscleanuptool_x86.exe

b/ Exécutez le fichier d'installation :

- l'outil crée un point de restauration du système avant d'effectuer la désinstallation ;
- lisez l'avertissement ;
- acceptez le CLUF, puis cliquez sur « J'accepte » pour commencer l'installation.

c/ Cliquez sur « Analyser » pour rechercher les produits de sécurité Internet Comodo. Lorsque l'outil détecte des produits spécifiés, cliquez sur « Continuer » pour les supprimer.

d/ Cliquez sur « Redémarrer » une fois le processus de nettoyage terminé. L'outil nécessite un deuxième redémarrage pour finaliser la suppression . »

18 Mesures générales de sécurité

Au niveau du pare-feu il faut rappeler qu'il est nécessaire :

1/ d'analyser régulièrement « Intrusions réseaux » afin de vérifier qu'une application essentielle, comme celles relevant d'un antivirus, n'a pas été bloquée et afin de repérer une éventuelle attaque ;
2/ de ne jamais autoriser une demande de connexion entrante ;

3/ de sécuriser le pare-feu en choisissant et paramétrant l'un des trois niveaux de sécurité exposés dans le second tutoriel [2] :
- ceux qui ne désirent pas s'impliquer outre mesure dans la gestion du pare-feu pourront se contenter de choisir le niveau 1 de sécurité en consultant et mettant en œuvre les paragraphes 8.2 et 9 de ce second tutoriel ;
- ceux qui souhaitent davantage de sécurité pourront s'intéresser à l'ensemble de ce second tutoriel et notamment au paragraphe 1 qui résume le fonctionnement du trafic sur Internet et sur le réseau local.

4/ de ne jamais oublier que la protection assurée par un pare-feu ne résout pas tous les problèmes de sécurité : voir ci-dessous

Rappelons que les principaux dangers proviennent :

- de la box : réglez-la en mode routeur ; désactivez le ping et, si possible, UPnP ; utilisez les Freebox WPA3-AES (dès le 14/07/2020), à défaut mettez la WiFi en WPA2-AES, avec un mot de passe fort pour la clef (au moins 16 caractères avec minuscules, majuscules, chiffres et caractères spéciaux), et masquez le réseau WiFi dans la box ;
- du Web : **connectez-vous avec un compte utilisateur**, jamais avec le compte administrateur ; **utilisez un navigateur sécurisé tel Firefox, Comodo Ice Dragon ou Comodo Dragon dans le conteneur** ;
- de la Wi-Fi à l'extérieur : utilisez-la avec prudence ;
- des achats en ligne : privilégiez le paiement par e-carte bancaire ;
- de la messagerie : n'ouvrez pas les pièces jointes inconnues ; évitez les messageries qui ne respectent pas la confidentialité, comme G-Mail ;
- de mots de passe insuffisamment robustes ;
- des clefs USB et CD : analysez-les avec votre antivirus avant de les employer ;

et, comme nous le verrons en [2] :

- des objets connectés et smartphones, particulièrement s'ils ne sont pas sécurisés ;
- des imprimantes connectées en Wi-Fi (par commodité ou pour l'envoi d'encre) ;
- des partages : les éviter ou les sécuriser.

Bonne route à vous sur les chemins du Web

Bibliographie

[1] « **Comodo Internet Security, version 12** », 688 p, manuel de l'utilisateur ;

- à consulter, notamment les appendices en fin de manuel ; en anglais :

https://help.comodo.com/uploads/helpers/Comodo_Internet_Security_ver.12.0_User_Guide.pdf

[2] Dumontet Michel « **Tutoriel COMODO Internet Security : 2/ Gestion sécurisée du pare-feu (alertes, règles et journal)** », Ed 02, 83 p. , Forum français de Comodo, septembre 2020.

[3] Legand Patrick **« Sécuriser enfin son PC »**, Groupe Eyrolles, 400 p. , Paris, 2007.

- une bonne introduction à la sécurité informatique pour les néophytes et les autres

[4] Lalitte Eric **« Apprenez le fonctionnement des réseaux TCP/IP »**, 3ème édition, 289 p., Eyrolles, Paris, 2018,

- pour débuter l'étude de TCP/IP, à compléter par l'ouvrage suivant ;

[5] Fall Kevin R. , Stevens W. Richard **« Tcp/Ip Illustrated : The Protocols »**, Volume 1, 2nd Edition, 963 p. , Pearson Education, 2012,

- un grand classique : les fondamentaux du système IP et des protocoles associés ; certaines parties d'un niveau élevé ;

[6] Cheswick William R., Bellovin Steven M. , Rubin Aviel D. **« Firewalls and Internet Security »** 2nd Ed., 397 p. , Pearson Education, 2003,

- un ouvrage de référence ;

[7] Zwicky Elizabeth D., Cooper Simon & Chapman D. Brent **« Building Internet Firewalls »** 2nd Ed. 890 p. , O'Reilly & Associates Inc. , June 2000 ;

[8] « **Désactiver les services inutiles de Windows 7** » PCAstuces :

https://www.pcastuces.com/pratique/windows/services_windows7/page1.htm

[9] « **Désactiver les services inutiles de Windows 8.1** » PCAstuces :

https://www.pcastuces.com/pratique/windows/services_windows_81/page1.htm

[10] « **Optimiser Windows 10 : les services Windows à désactiver** » :

https://www.malekal.com/optimiser-windows-10-les-services-windows-a-desactiver/

[11] « **Comodo IceDragon, version 65.0** » **;** Manuel d'utilisation en anglais, 189 p. :

https://help.comodo.com/uploads/helpers/Comodo%20IceDragon%20ver.65.0%20User%20Guide.pdf

[12] « **Comodo Dragon, version 80 .0** » **;** Manuel d'utilisation en anglais, 186 p. :

https://help.comodo.com/uploads/helpers/Comodo_Dragon_Web_Browser_ver.80.0_User%20Guide.pdf

[13] Forum français de Comodo

https://forums.comodo.com/francais-french-b72.0/

[14] Outil de désinstallation de Comodo

https://help.comodo.com/topic-72-1-766-12685-Use-the-Comodo-Uninstaller-Tool.html