Tutoriel COMODO Internet Security
2/ Gestion sécurisée du pare-feu (alertes, règles et journal) Ed 02

Ed 02 : Rédacteur : Michel Dumontet d : 18/09/2020

Table des matières

Ce tutoriel fait suite au « **Tutoriel de COMODO Firewall et de Comodo Internet Security 1/ Installation et configuration. » [1],** qu'il complète.

Rappelons que Comodo Firewall peut être employé associé, au sein de Free Internet Security, à l'antivirus de Comodo, ou à tout autre antivirus du marché [1].

Firewall, est un pare-feu particulièrement performant et riche en fonctionnalités, comportant notamment :

a/ un module pare-feu proprement dit qui contrôle le trafic des paquets d'informations entre votre ordinateur et les réseaux Internet et local, **trafic dont nous allons étudier la gestion dans ce tutoriel** ;

b/ un très intéressant **conteneur (sandbox ou bac à sable)**, où sont automatiquement exécutées les applications inconnues ou douteuses, et dans lequel vous pouvez, si vous le désirez, ouvrir, Facebook, Twitter, votre messagerie, vos navigateurs Firefox, Dragon, IceDragon qui peuvent ainsi vous permettre de surfer sur le Web en demeurant protégés d'éventuels maliciels (malwares) ;

c/ des modules HIPS (Host Intrusion Prevention System), **Viruscope et de filtrage des sites Web** qui complètent la protection de l'ordinateur (voir [1] 8.2.3 & 8.2.4.

Ce tutoriel venant compléter le tutoriel précédent nous n'y aborderons que la configuration du seul module pare-feu.

Les utilisateurs qui ne désirent pas s'impliquer dans la gestion du pare-feu pourront se contenter de lire rapidement les paragraphes 2 à 7, ainsi que 13, de privilégier la lecture du paragraphe 9, et de consacrer environ une demi-heure à la mise en place du Niveau 1 de sécurité assurant ainsi la sécurisation minimale essentielle du pare-feu qui fonctionnera ensuite en mode sécurisé quasi automatique.

Par contre, les utilisateurs qui désirent avoir une meilleure compréhension de la gestion du pare-feu et s'impliquer davantage dans cette gestion pourront consulter l'ensemble du tutoriel. Nous avons rassemblé dans le premier paragraphe, de la façon la plus accessible possible, les principaux éléments concernant les modalités du trafic Internet ; toutefois ne vous inquiétez pas si vous ne comprenez qu'incomplètement : vous comprendrez mieux en poursuivant la lecture du tutoriel ou lorsque vous rencontrerez les situations décrites ; enfin vous pourrez approfondir vos connaissances en consultant certains des ouvrages mentionnés en bibliographie.

1 Fonctionnement du trafic sur Internet et sur le réseau local

A*u travers de ses 65 635 ports, chaque ordinateur est capable d'établir des connexions afin d'échanger des paquets d'informations avec des ordinateurs du monde entier ;*
le réseau de communication Internet est constitué d'une multitude de routeurs qui se transmettent de proche en proche les paquets qu'ils acheminent jusqu'aux ordinateurs destinataires.

1.1 Les différents groupes de ports

Les ports ont été classés par l'IANA (Internet Assigned Number Authority) en :

a/ ports « bien connus » (well-known ports ou ports du système) de 0 à 1023, affectés aux services réseaux les plus courants : leur utilisation par le logiciel serveur* nécessite souvent que celui-ci dispose des privilèges de super-utilisateur ;

b/ ports « enregistrés » (registered ports) de 1024 à 49151 qui peuvent être utilisés sans privilège de super-utilisateur ;

c/ ports « dynamiques », de 49152 à 65535, utilisés à des fins privées, à des services sur mesure, à des besoins temporaires et pour l'allocation automatique des ports utilisés de façon éphémère.

Les ports « bien connus » et les ports « enregistrés » sont principalement utilisés par les programmes serveurs* ; les ports « dynamiques » par les programmes clients* ;

note* : programmes serveurs et clients ci-dessous explicités.

1.2 Environnement « client-serveur »

L'environnement « client-serveur » désigne un mode de communication entre plusieurs programmes sur un réseau (note : la version française de Comodo emploie indifféremment les termes programmes ou applications).

Le programme serveur (ou par extension l'ordinateur serveur) offre, par l'intermédiaire d'un protocole, un service : par exemple un serveur Web vous propose des pages Web, un serveur de messagerie vous permet d'envoyer et de recevoir des courriels (e-mails), etc...

Il est donc nécessaire que ce serveur puisse être joint à tout moment par les internautes clients et attende, afin de pouvoir y répondre, les requêtes de connexions entrantes sur un ou plusieurs ports **en écoute** de l'ordinateur sur lequel il est hébergé ; aussi l'IANA a-t-elle affecté à chaque type de protocole un port ou des ports de la série des ports de 0 à 1023 (ports dits «bien connus »), par exemple :
- le port 80 pour le protocole HTTP et le port 443 pour le protocole sécurisé HTTPS des services Web ;
- le port 53 pour le protocole DNS des serveurs DNS, etc... ;
ainsi un serveur Web laissera-t-il ses ports 80 (protocole HTTP) et 443 (protocole HTTPS) en attente des requêtes provenant des navigateurs des ordinateurs des internautes clients ;

Le programme client (ou par extension l'ordinateur client) envoie, sous forme de paquets, une requête de connexion à destination du port en écoute du serveur qu'il désire consulter ; lorsqu'une requête de connexion arrive sur le port en écoute, une interface de connexion va être ouverte sur l'ordinateur serveur, interface par laquelle la communication avec le client sera établie selon le protocole prévu par la couche applications du modèle TCP-IP (cf. 1.4.7).

1.3 Paquets et système de notation des adresses

1.3.1 Les paquets

Lors d'une communication sur un réseau, des paquets (datagrammes) sont acheminés sous forme de signaux, représentés par des bits (abréviation de **bi**nary digi**t ;** le bit ne peut prendre que les deux valeurs 0 et 1).

Chaque paquet comprend un contenu, le corps, et des en-têtes : le paquet contient ainsi plusieurs informations, dont les adresses source et de destination et le protocole de transmission (TCP, UDP, ICMP …) qui permettent d'assurer son acheminement, de routeur en routeur, jusqu'à sa destination finale (cf. 1.5).

1.3.2 L'adresse MAC

Chaque objet connecté (ordinateur, imprimante, etc.) est équipé d'une carte Ethernet, pourvue d'une adresse MAC, unique au monde, qui permet l'identification de la machine correspondante (cf. 1.4.2).

L'adresse MAC est utilisée sur le réseau local ; elle occupe 48 bits segmentés en

six champs de huit bits (octets), elle peut donc prendre 2 puissance 48 valeurs, soit environ 256 mille milliards d'adresses MAC, on ne risque donc pas d'avoir une pénurie d'adresses MAC !

Une adresse MAC ne s'exprime pas en langage décimal de dix chiffres de 0 à 9, mais en langage hexadécimal, c'est à dire sous forme de 16 chiffres de 0 à 9, a, b, c, d, e , f ; par exemple : **02:28:5d:bf:52:8a**

1.3.3 L'adresse IP

Pour des raisons techniques on n'emploie pas les adresses MAC sur le réseau Internet, mais les adresses IP (Internet Protcol). Une partie de l'adresse correspond à l'identification du réseau, et l'autre à l'identification de la machine.

Avec le protocole IPv4, le plus utilisé actuellement, une adresse IPv4 occupe 32 bits segmentés en quatre champs de huit bits (octets) : l'adresse IPv4 est donc composée de 32 chiffres 0 ou 1 consécutifs. Ceci étant peu maniable, chacun de ces octets est converti en un nombre décimal compris entre 0 et 255, et séparé du précédent par un point ; ce qui donne, en IP v4, des adresses sous la forme « xxx.xxx.xxx.xxx », par exemple, **169.229.131.81** (adresse de l'université de Berkeley).
L'adresse Ipv4 étant codée sur 32 bits peut prendre 2 puissance 32 valeurs, soit environ 4 milliards d'adresses, ce qui est peu, relativement à l'explosion du nombre d'objets connectés.

Aussi, afin de prévenir une pénurie d'adresses Ipv4, a-t-on mis en place deux solutions :
- la plus ancienne, temporaire, mais actuellement la plus utilisée, est la **« translation d'adresses »** (Network Adress Translation ou **NAT**) : voir ci-dessous 1.3.4 ;
- la plus récente consiste à remplacer progressivement le protocole Ipv4 par le protocole Ipv6, une adresse Ipv6 occupant 128 bits au lieu de 32 bits, ce qui augmente considérablement le nombre d'adresses disponibles.

1.3.4 Les adresses publiques et privées ; la translation d'adresses NAT

Les **adresses publiques,** utilisables sur Internet, sont gérées par un organisme public, l'ICANN, qui les attribue aux divers fournisseurs d'accès Internet. Lorsque vous vous abonnez auprès de l'un d'eux, celui-ci vous loue une box avec une seule de ces adresses publiques.

Les adresses privées sont attribuées, de manière temporaire ou fixe, à chacun des équipements connectés du réseau local [ordinateur(s), imprimante(s), etc...] disposant d'une adresse MAC :
- directement par le serveur DHCP d'un routeur, ici celui de la box fonctionnant en tant que routeur ;
- par encodage manuel par l'utilisateur au niveau de la box (cf. Annexe A 1.1) ;
- à défaut des deux processus précédents, par le système d'exploitation qui fournit alors une adresse, dite APIPA, comprise entre 169.254.0.0 et 169.254.255.255

Les adresses privées ne sont pas utilisables sur Internet (on dit qu'elles ne sont pas routables) ; elles doivent être choisies dans les plages d'adresses réservées :
- 10.0.0.0 à 10.255.255.255 ;
- 172.16.0.0 à 172.31.255.255 ;
- 192.168.0.0 à 192.168.255.255 ;

La fonction NAT dynamique, dans un routeur, ou une box fonctionnant en tant que routeur, est chargée de faire correspondre la seule adresse publique du routeur ou de la box, accessible sur Internet, à chacune des adresses privées des équipements connectés du réseau local.

Ainsi peut-on théoriquement relier à une seule adresse publique jusqu'à 6 000 adresses privées, ce qui prévient la pénurie d'adresses IP. Par ailleurs ceci permet que les adresses privées ne soient pas visibles sur Internet, ce qui accroît la sécurité.

Lors de la requête de connexion la box attribuera un port source, privé ou dynamique (de 49152 à 65535), à l'adresse IP de l'équipement demandeur source et conservera dans la table NAT cette association entre l'adresse IP source et le port source. Elle substituera ensuite l'adresse privée par son unique adresse publique, ce qui lui permet d'envoyer le paquet sur le réseau Internet. Lorsque la réponse du site destinataire arrivera en direction du port source, la table NAT permettra d'acheminer la réponse vers l'adresse de l'équipement demandeur source associée à ce port source (pour plus de détails cf. [5], chapitre 13).

1.3.5 Les diffusions unicast, broadcast et multicast

- unicast (diffusion unique) **: transmission, sur le réseau IP, des paquets d'un hôte (machine) unique vers un seul autre hôte** ; c'est le type de liaison couramment employé, par exemple lors de la communication entre deux ordinateurs (l'un celui du client, l'autre celui du routeur) identifiés chacun par une adresse réseau unique, par

exemple de **192.168.0.14** vers **169.229.131.81** ;

- broadcast : diffusion d'un hôte vers l'ensemble des machines d'un réseau local ; c'est le type de diffusion utilisé pour atteindre une machine dont on ne connaît pas l'adresse MAC, par exemple par une requête d'un ordinateur envoyée vers le serveur DHCP de sa box (cf. 1.4.2 et 1.4.7 e/). Les routeurs (ou box-routeurs) ne diffusent pas sur le réseau Internet les paquets qui demeurent donc cantonnés au réseau local ;

- **multicast** (multidiffusion ou diffusion de groupe) : **diffusion d'un hôte vers l'ensemble des machines inscrites à un groupe de diffusion ;** le même paquet, émis une seule fois, est routé [acheminé sur le réseau Internet de routeur en routeur jusqu'au(x) destinataire(s)] à toutes les machines du groupe de diffusion ; ceci est classiquement utilisé pour l'envoi du même document aux divers membres d'un groupe de diffusion, ou plus récemment pour la diffusion de programmes radiophoniques, télévisés, de cours à distance, etc.

1.3.6 Les adresses des sites Web et le protocole DNS

Chaque site Web est pourvu d'une adresse publique, en Ipv4 sous la forme « xxx.xxx.xxx.xxx » où « xxx » est un nombre compris entre 0 et 256 qui l'identifie sur le réseau, par exemple 169.229.131.81 pour l'université de Berkeley.

Afin de faciliter l'accès des utilisateurs aux sites Web, l'adresse IP numérique ci-dessus est associée à un nom plus aisé à retenir, « le nom de domaine », qui sera utilisé dans la barre d'adresse de votre navigateur, par exemple ci-dessus https://www.berkeley.edu pour l'adresse IP 169.229.131.81 de ladite université de Berkeley.

Votre ordinateur s'adressera alors à un serveur DNS, en général l'un de ceux de votre fournisseur d'accès Internet, qui résoudra, selon le protocole DNS, ce nom de domaine, c'est-à-dire qui le traduira en son adresse numérique, seule identifiable sur le réseau Internet.

Malheureusement le protocole DNS est peu sécurisé et plusieurs failles de sécurité ont été identifiées. Nous avons vu, lors de l'installation du pare-feu [1], que Comodo propose de remplacer les serveurs DNS du fournisseur d'accès Internet par ses propres serveurs Comodo Secure DNS et nous verrons, par ailleurs, comment limiter le détournement de DNS au moyen de deux règles globales d'autorisation des connexions en direction du port 53 pour les seules destinations des deux serveurs mis à disposition par Comodo dont les adresses, en France métropolitaine, sont 156.154.70.25 et 156.154.71.25 (cf. 11.1 b/).

1.3.7 Les protocoles m-DNS et LLMNR

m-DNS (Multicast DNS), développé par Apple, qui utilise le port **UDP 5353** et **LLMNR** (Link-Local Multicast Name Resolution), développé par Microsoft, qui utilise le port **UDP 5355** sont des protocoles proches du protocole DNS et qui jouent le même rôle de résolution de noms, mais pour le nombre restreint d'hôtes d'un réseau local : sur votre réseau local ils peuvent assurer notamment la communication entre vos ordinateurs et vos imprimantes (cf : 11.2.3 B/ b/).

1.3.8 L'adresse IP 127.0.0.1 (appelée **en anglais loopback adress ou localhost)**

Quoique cela puisse paraître inattendu d'assez nombreuses applications souhaitent envoyer un signal qui sera renvoyé sur leur émetteur, à titre de test par exemple. Il s'agit donc d'un « loopback » (bouclage arrière), intitulé dans la traduction française de Comodo « accès à la boucle locale », qui utilise, en Ipv4, l'adresse IP 127.0.0.1, celle-ci n'étant pas routable sur le réseau Internet (ce trafic en boucle ne quitte jamais la machine).

Afin de ne pas perturber le fonctionnement optimal de ces applications il sera nécessaire d'autoriser ces demandes d'accès à la boucle locale qui sont du type : **« TCP sortant de 127.0.0.1 vers 127.0.0.1 »** ; les ports sources et destinataires utilisés se situent dans la plage des ports dynamiques de 49152 à 65535 et sont très nombreux pour la même application, ce dont tiennent compte les règles prédéfinies « Navigateur Internet » et « Client de messagerie » (et, pour la seule gestion personnalisée, une règle prédéfinie « Application limitée autorisée » que nous créerons (cf. Règles prédéfinies : 10.1).

1.4 Modèles OSI et TCP-IP

Le modèle OSI est un modèle théorique qui décompose les différents protocoles de communication en sept couches, chacune étant responsable d'un aspect particulier de la communication.

Le modèle TCP/IP rassemble l'ensemble des protocoles utilisés pour le transfert des données sur Internet : il a été partiellement repris du modèle OSI. Chaque couche traite de problèmes spécifiques et fournit des services définis aux couche supérieures.

1.4.1 - couche **1. Physique** : cette couche spécifie notamment les supports de communication (câbles Ethernet, fibre optique ou ondes radio, en mode Wi-Fi), utilisés pour la communication entre votre box et les appareils à connecter ;

1.4.2 - couche **2. Liaison de données** : cette couche spécifie les moyens et méthodes qui permettent la communication entre les objets connectés du réseau local :

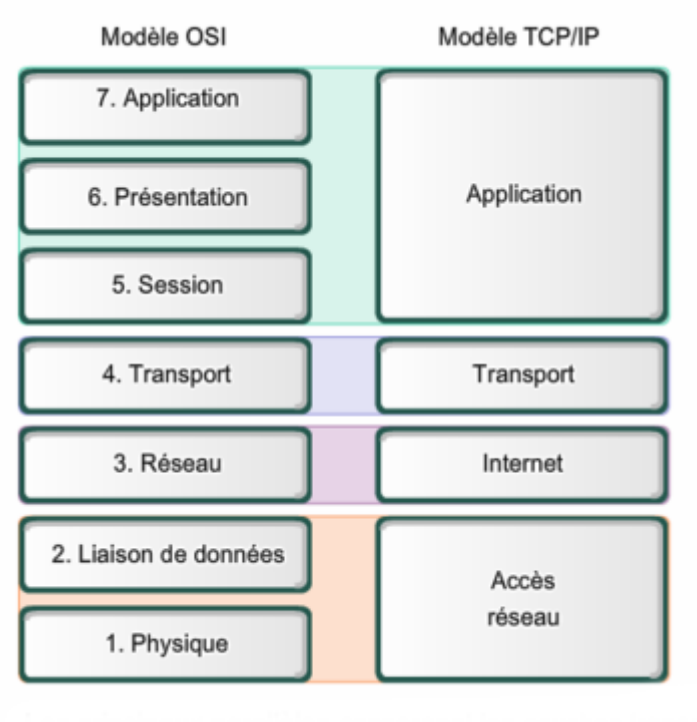


schéma et texte d'après d'après Wikipedia

= chaque objet connecté (ordinateur, imprimante, etc.) est équipé d'une carte Ethernet, pourvue d'une adresse MAC, unique au monde, qui permet l'identification de la machine correspondante ;
= par ailleurs ces machines sont reliées entre elles par un commutateur (switch en anglais), qui est désormais le plus souvent inclus dans une box ;
= enfin la communication se fait selon le protocole Ethernet ou le protocole Wi-Fi qui définissent quelles informations véhiculées dans la trame internet sur le réseau local doivent être utilisées et de quelle manière.
= il faut distinguer une adresse MAC particulière : l'adresse de broadcast ou adresse universelle (ff:ff:ff:ff:ff:ff) qui identifie n'importe quelle carte Ethernet et permet ainsi de s'adresser en une seule fois à toutes les adresses du réseau local ;

1.4.3 - couche **2,5** : sur cette couche intermédiaire, non officielle, on trouve **le protocole ARP** (Address Resolution Protocol) qui permet d'établir un lien entre l'adresse MAC, de couche 2, d'un équipement et son adresse IP, de couche 3, au moyen d'une table ARP de correspondance entre ces deux type d'adresses. Le protocole ARP permet ainsi de mettre à jour les changements intervenus sur le réseau local, par exemple lors du remplacement d'une carte Ethernet sur un ordinateur du

réseau ; son emploi est donc particulièrement pertinent dans un réseau local comprenant de nombreuses machines qui doivent rester à jour ; par contre son emploi l'est beaucoup moins pour un seul ordinateur de votre réseau local [2], aussi est-il préférable, dans ce cas, d'activer l'anti-usurpation d'identité (cf. 5.1 d/) car la table ARP peut être modifiée à distance par un pirate lors d'une attaque « ARP cache poisonning » ; les blocages de connexions ARP (pour Windows Operating System) apparaîtront alors dans le journal du pare-feu ;

1.4.4 - couche **3. Réseau** : sur la couche Réseau on trouve **IP (Internet Protocol),** sous la version Ipv4 ou IP v6 ; c'est le protocole principal du modèle TCP/IP **qui assure notamment l'adressage et le routage des paquets** entre les divers hôtes ; le format et la structure standard des paquets véhiculés sur le réseau Internet (IP datagram) sont notamment décrits dans ce protocole :
= IP, cependant, n'apporte pas de garantie sur l'ordre d'arrivée des paquets, leur perte, leur destruction ou leur duplication lors de leur acheminement ; pour ce faire, IP est assisté par les protocoles TCP de la couche Transport (couche 4) : *cf [4], [5], [6], [7] & [8] pour plus de détails sur le modèle TCP/IP ;*
= IP peut également être assisté des protocoles ICMP et IGMP : voir ci-dessous

1.4.5 - couche **3.5** : sur cette couche intermédiaire, également non officielle, on trouve notamment les protocoles d 'administration *ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Control),* qui peuvent être utilisés par les administrateurs de réseaux locaux relativement importants ; *mais ils peuvent également être utilisés par des pirates pour explorer la structure d'un réseau local sur lequel ils désireraient s'introduire :* **si votre ordinateur est isolé ou fait partie d'un simple réseau domestique ou d'un réseau plus important dont l'administrateur n'utilise pas ces protocoles, il est préférable de bloquer les connexions entrantes et sortantes de ces protocoles** (cf. 9.2).

1.4.6 - couche **4. Transport :** sur la couche Transport nous trouvons les protocoles **TCP (Transmission Control Protocol), et UDP (User Datagram Protocol)** qui assistent IP dans l'acheminement des paquets :

= TCP est un protocole de transport complexe dit « fiable » car il assure l'arrivée à destination des paquets envoyés, sans altération et dans l'ordre d'envoi, ainsi que la récupération des paquets perdus au cours de la transmission ;

= **UDP est un protocole de transport simple dit « non fiable »** car il ne vérifie pas que les paquets sont arrivés à destination, ni qu'ils sont arrivés dans l'ordre d'envoi ; il

est utilisé pour sa rapidité par des applications qui n'ont pas besoin de ces garanties ou qui les assurent elles-mêmes.

1.4.7 - couche Applications : la couche Applications fournit à de nombreux protocoles la possibilité d'accéder aux services des autres couches ; nous rencontrerons souvent les protocoles:

a/ HTTP (Hypertext Transfert Protocol), associé au port 80, et **HTTPS**, sa forme sécurisée, associé au port 443, tous deux employés par les navigateurs pour transmettre les fichiers des pages Web ;

b/ DNS (Domain Name System), employé pour la résolution des noms de domaines en adresses IP (cf. 1.3.6 ci-dessus) ;

c/ SMTP (Simple Mail Transfert Protocol), associé au port 25 non crypté, ou au port 587 (ou 465) pour un emploi sécurisé, protocole standard **pour l'envoi** de courriers électroniques sur Internet ;

d/ POP3 (Post Office Protocol, version 3), associé au port 110 non crypté, ou au port 995 pour un emploi sécurisé, ou **IMAP (Internet Message Access Protocol)**, associé au port 143 non crypté, ou au port 993 pour un emploi sécurisé, tous deux protocoles de messagerie Internet utilisés **pour la récupération** des courriers électroniques sur votre ordinateur à l'aide d'un Client de Messagerie tel Thunderbird ;

e/ DHCP (Dynamic Host Configuration Protocol), protocole permettant à un serveur DHCP, celui de la box (configurée en mode routeur) ou celui d'un routeur, d'attribuer de manière dynamique (automatique), pendant un certain temps (bail), une adresse IP privée aux machines d'un réseau local, ainsi que les adresses DNS, permettant à ces machines de se connecter à Internet par l'intermédiaire de cette box ; lorsque le bail d'une machine a expiré, elle n'a plus d'adresse IP valide, aussi initie-t-elle une série d'échanges avec le serveur DHCP de sa box en employant l'adresse factice 0.0.0.0 pour envoyer une requête (DHCPDISCOVER) au-dit serveur DHCP sous la forme : « **de 0.0.0.0, port 68, vers 255.255.255.255, port 67** », où 255.255.255.255 est l'adresse de broadcast (cf. 1.3.5).

Ce protocole a été mis au point afin d'éviter notamment une lourde charge de travail aux administrateurs de réseaux locaux importants.

Cependant le service DHCP peut être cible d'attaques, par exemple de type « DHCP Starvation » ou « DHCP Rogue ». Aussi, pour les réseaux locaux de moins d'une trentaine d'ordinateurs fixes, est-il préférable de revenir à l'adressage statique (IP fixes) originel : il suffit que l'utilisateur fasse correspondre dans la table adéquate de sa box, l'adresse MAC de chacun de ses équipements à une adresse privée déterminée (cf. Annexe A - Centre Réseau et partage A.1 Désactiver DHCP) ; par ailleurs, cela rendra plus aisé, au niveau du pare-feu, l'attribution sélective à quelques équipements de règles particulières d'autorisation ou de blocage.

f/ SMB (Server Message Block) est le protocole de partage des fichiers et imprimantes sur des réseaux locaux sous Windows ; il utilise TCP sur le port 445 et existe en plusieurs versions (SMB1, SMB2 et SMB3). Sur les systèmes Windows postérieurs à février 2000 il peut être utilisé sans l'assistance de Netbios qui pose de graves problèmes de sécurité ; mais, même ainsi, il peut présenter des failles de sécurité (on a encore découvert, le 10 mars 2020, la faille SMBGhost sur SMBv3 permettant à des vers informatiques d'infecter les PC) ; il est donc souhaitable :
- de désactiver les partages non indispensables ou de sécuriser ceux qui le sont (cf. Annexe 4) ; de désactiver SMBv1 (cf. Annexe 5) ;
- de bloquer les connexions pour SMB (TCP, port 445) au niveau du pare-feu ou, si les partages vous sont indispensables, de n'autoriser que les connexions sortantes pour SMB sur le seul réseau local (cf. 9.3.1) ;

g/ Système Netbios : le système Netbios assiste le système SMB **pour assurer la gestion des partages de fichiers et d'imprimantes** ; il utilise les ports UDP 137 et 138 et le port TCP 139 ; il est très peu sécurisé et constitue, ainsi que le service de localisation pour les appels de procédure distante sur le port 135, **une très grave faille de sécurité**, de plus SMB n'a désormais plus besoin de l'assistance du Système Netbios. Aussi le système Netbios doit-il être désactivé dans Windows (cf. Annexe A.3 Désactiver Netbios) et les demandes de connexions le concernant doivent-elles être bloquées au niveau du pare-feu (cf. 9.3 f/) car, bien que désactivé, il est parfois malencontreusement réactivé dans Windows.

h/ SSDP (Simple Service Discovery Protocol) est un protocole qui permet de découvrir des services disponibles sur le réseau ; il est utilisé comme base par UPnP (Universal Plug and Play) afin de « faciliter l'installation, la configuration et l'ajout de périphériques informatiques à un micro-ordinateur » (Wikipedia). Il utilise UDP sur le port 1900 en unicast ou en multicast. Les dispositifs UPnP disponibles répondent en lançant une connexion TCP sur le port 5000, ce qui initie le dialogue entre les périphériques concernés ; SSDP est utilisé pour les partages sur Windows Media

(Player).

Malheureusement le protocole UPnP comporte de très nombreuses failles de sécurité et peut permettre à des pirates d'inclure votre ordinateur dans un botnet afin de perpétrer des attaques massives d'autres ordinateurs par déni de service, aussi est-il prudent et souhaitable de désactiver SSDP, l'Hôte de périphérique UpnP et Service Partage réseau du Lecteur Windows Media (cf. Annexe B - Gestion des services Windows) et de bloquer les demandes de connexions vers le port UDP 1900 (cf. 9.3). Il sera toujours possible de revenir sur ces réglages s'il s'avéraient nécessaires pour l'installation d'un équipement particulier.

i/ SNMP (Simple Network Management Protocol) est un protocole de gestion principalement utilisé par les administrateurs des grands systèmes pour superviser à distance les équipements informatiques. Nous ne l'avons rencontré que dans le cadre de la gestion par HP de l'approvisionnement en encre de notre imprimante HP. Il utilise UDP sur les ports 161 et 162. Il est si peu sécurisé (« Security is Not My Problem » disent les méchantes langues) que Windows l'a enfin retiré de ses fonctionnalités depuis Windows 10 1809. Il est indispensable de le désactiver sur les versions antérieures de Windows (cf. Annexe B : Gestion des services Windows) et de bloquer les demandes de connexions sortantes en direction des ports UDP 161 et 162 (cf. 9.3).

j/ FTP (File Transfer Protocol) : « Le protocole de transfert de fichiers » est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. » (Wikipedia). Si vous ne désirez pas ouvrir votre ordinateur à tous vents il est fondamental de spécifier les adresses destination et source dans les règles créées à l'usage de FTP (cf. [4] pp. 185-186 et les règles prédéfinies en 10.1.1 c/) ; ceux qui désirent utiliser ce protocole trouveront des explications sur ses dangers et sur les précautions à prendre dans [7] pp. 287-295 et [8] pp. 53-57.

1.5 Formation et acheminement du datagramme ou paquet

Les données circulent sur Internet sous forme de datagrammes (ou paquets au sens large du terme) :
- les données du message initial de la machine émettrice sont élaborées par l'application située sur la couche « Applications » du modèle OSI ou TCP/IP : elles constituent **le corps** du futur datagramme ;

- celui-ci va traverser de haut en bas la pile des diverses couches du modèle OSI (ou du modèle TCP) : chaque couche va ajouter au corps, par encapsulations successives, une information sous forme d'en-tête, jusqu'à l'obtention du datagramme de la couche 2 qui sera transmis, sur Internet, de routeur en routeur jusqu'à sa destination finale grâce aux informations collectées dans les en-têtes, notamment :
  - **les adresses source et de destination**, comme sur un courrier postal ;
  - **l'identification** ;
  - **le protocole de transmission** (TCP, UDP, ICMP …) ;
  - **la somme de contrôle de l'en-tête**, résultat d'un calcul qui permettra de vérifier l'intégrité globale de l'en-tête ;
  - **la durée de vie** (Time to Live ou TTL) qui indique le nombre maximal de routeurs de transit ;
- arrivé à destination sur la machine réceptrice, le datagramme suivra le chemin inverse : il remontera, grâce aux informations contenues, les couches de la pile OSI, jusqu'à l'application émettrice concernée.

1.6 Paquets fragmentés

Un paquet de taille supérieure à l'« Unité de Transmission Maximale » est fragmenté, pour le transport, en paquets plus petits, puis est ré-assemblé par le destinataire ; malheureusement ces paquets IP fragmentés peuvent être utilisés à des fins malveillantes, aussi leur trafic doit-il, en général, être bloqué (cf. 5.1 c/).

Toutefois le trafic des paquets fragmentés ne doit pas être bloqué si vous utilisez des applications audio ou vidéo de haute qualité qui fragmentent les paquets IP, ainsi que lors de l'utilisation de VPN, lors de certains jeux en ligne, ou si, par hasard, cela semble entraver une partie de votre trafic.

1.7 Danger des objets connectés

La majorité des milliards d'objets connectés n'est malheureusement pas ou mal sécurisée et ceux-ci partagent, chez les particuliers, le même réseau local que le ou les ordinateurs, permettant ainsi aux pirates de s'infiltrer dans toute l'installation. Aussi les experts en sécurité préconisent-ils de segmenter le plus possible le réseau local avec un routeur ou un routeur VPN (par exemple ASUS RT AC68U ou équivalent de Linskys ou autre) : d'un côté les équipements à hauts risques des enfants et adolescents, ainsi que les objets connectés, de l'autre le NAS et l'ordinateur parental qui n'admettra pas de connexions en provenance ou en direction du secteur à haut risque.

2 Connexions entrantes et connexions sortantes

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 (cf. 5.3 et 9.1)

- 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 les rendant 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, autant que possible, proscrire les connexions entrantes.**

Gestion des connexions sortantes (cf. 11.1)

- Une connexion sortante est lancée de l'intérieur de votre ordinateur en direction de l'extérieur ; une fois la connexion établie votre ordinateur peut aussi bien **exporter des données à l'extérieur qu'en importer ;**

- chaque fois qu'une application autorisée à se connecter sur Internet initie une session avec un ordinateur distant, le pare-feu laissera l'application ouvrir un port le temps de cette 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 ;

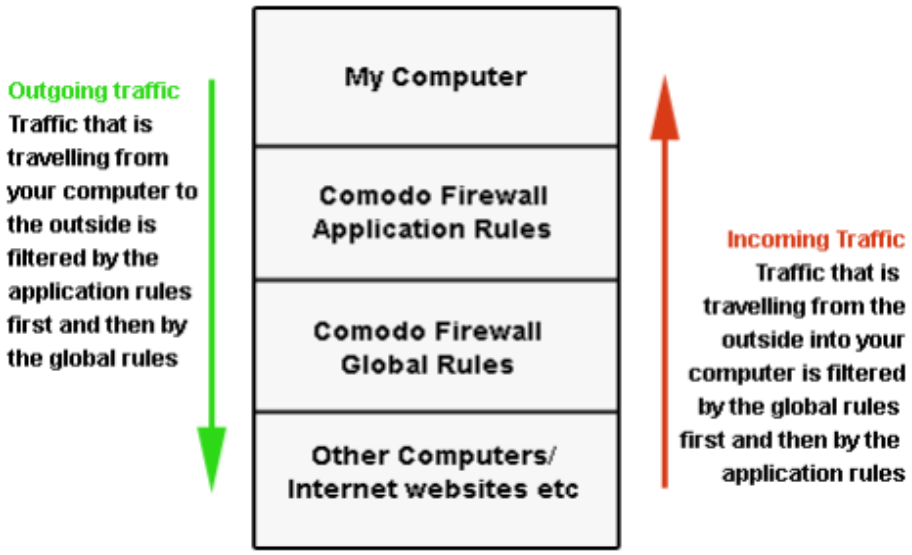
- afin d'assurer une sécurité optimale il est donc souhaitable de n'autoriser des connexions sortantes que pour des applications saines et qui vous sont indispensables.

3 Règles de programmes et règles globales

On 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 ; ainsi le pare-feu Comodo applique-t-il **un double filtrage des connexion** : l'un par les règles de programmes et l'autre par les règles globales :

- 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)

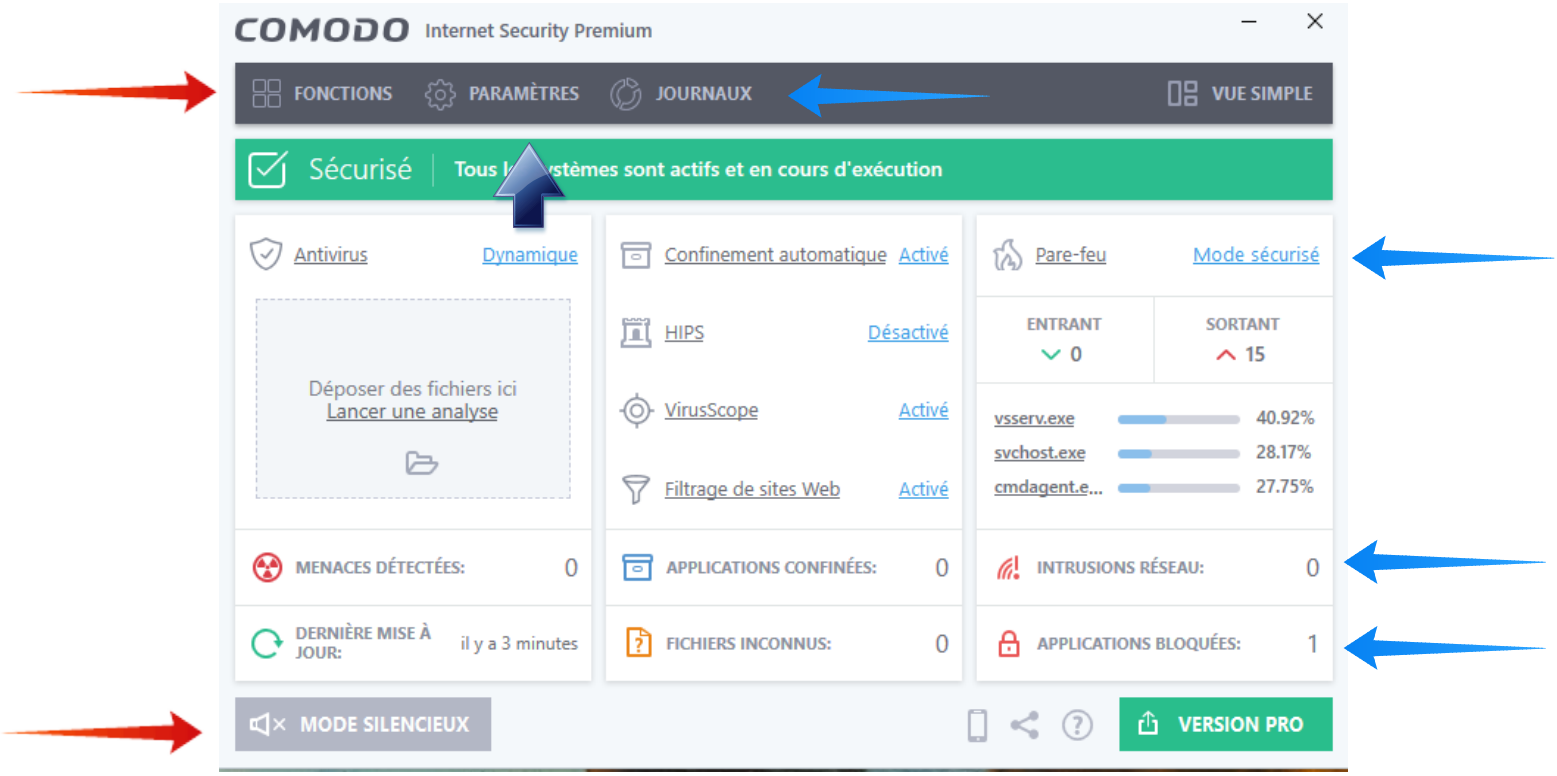
- à l'intérieur de la fenêtre des règles globales, une règle située en haut de cette fenêtre sera prioritaire sur les règles situées en dessous d'elle ;

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

4 La fenêtre d'accueil « Vue avancée » de la suite Comodo

Nous avons vu dans le tutoriel précédent comment accéder à cette fenêtre d'accueil:
- soit à partir de l'icône de la barre des tâches (clic gauche, puis cocher « Vue avancée », puis clic gauche sur « Ouvrir ») : voir [1] en 6.2 ;
- soit à partir de la fenêtre mobile en cliquant en haut, à gauche sur le pictogramme représentant une maison : voir [1] en 6.3,

Cette fenêtre d'accueil « Vue avancée », que vous trouverez ci-dessous, constitue la plaque tournante de la gestion de Comodo Firewall Free et de Comodo Free Internet Security. Pour ce qui est du pare-feu proprement dit, nous l'utiliserons pour accéder aux modules :



- « Paramètres » ;
- « Journaux ;
- « Fonctions », dont les « Fonctions du pare-feu » ;
- « Intrusions réseaux » et « Applications bloquées » ;
- « Mode sécurisé » ou « Mode personnalisé » du pare-feu ;
- enfin au « Mode silencieux » qui pourra être utilisé lors des jeux afin de ne pas être dérangé par une éventuelle alerte

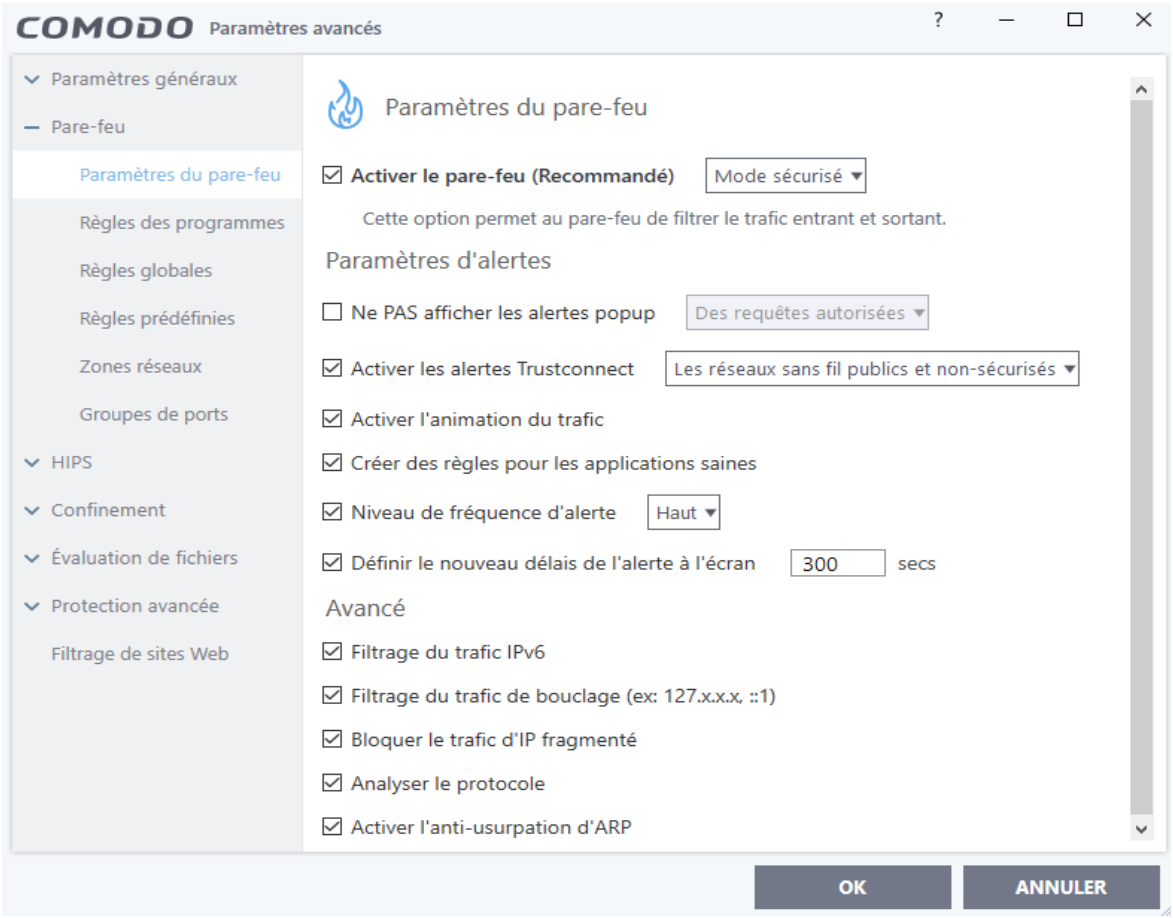
5 Configuration de base du pare-feu de Comodo

Cette configuration a déjà été présentée dans le tutoriel consacré à l'installation et à la configuration de CIS [1], particulièrement en 9.2, 10.2, 11 et 12 ;
les aspects les plus décisifs pour la sécurité de l'ordinateur étant abordés :
- en [1] 9.2 avec l'interdiction des connexions entrantes en provenance d'Internet, tout en cachant les ports ;
- en [1] 10.2 avec la présentation du pare-feu, de son paramétrage, des règles de programmes, globales et prédéfinies, des zones réseaux et des groupes de ports ;

- si l'on a déjà utilisé le pare-feu et créé des règles de programmes il est préférable de créer une nouvelle configuration ([1] 7.4) et de conserver l'ancienne en cas de besoin.

5.1 Configuration des paramètres du pare-feu

Nous préciserons seulement certains points particuliers concernant **le paramétrage de la configuration du pare-feu** (cf. [1]10.2.1) résumée dans la tableau ci-dessous :



a/ le pare-feu sera laissé en **mode sécurisé** lorsque l'on choisit le Niveau 1 de sécurité (cf. 9) et l'on optera ensuite pour le **mode personnalisé** lors du passage éventuel aux Niveaux 2 et 3 (cf. 10.3) et que les règles prédéfinies auront été aménagées à cet effet (cf. 10.1) ;

b/ si vous désirez consulter les règles de programmes appliquées, si vous souhaitez pouvoir éventuellement les modifier, les bloquer ou les classer en cours d'utilisation, il est nécessaire de cocher la case **« Créer des règles pour les applications saines »**.

c/ et il est alors important de passer le niveau de fréquence d'alerte **de « Bas » à « Haut »** , ce qui constitue un compromis équilibré assurant une bonne sécurité et une gestion aisée : les raisons de ce choix très important sont explicitées en 8.1 ;

d/ le trafic « IP fragmenté » **doit**, sauf cas particuliers (cf. 1.6), **être bloqué.**

e/ **Anti-usurpation d'ARP doit être activée**, sauf si votre réseau local comprend de nombreux ordinateurs (cf. 1.4.3)

5.2 Les « Zones réseaux »

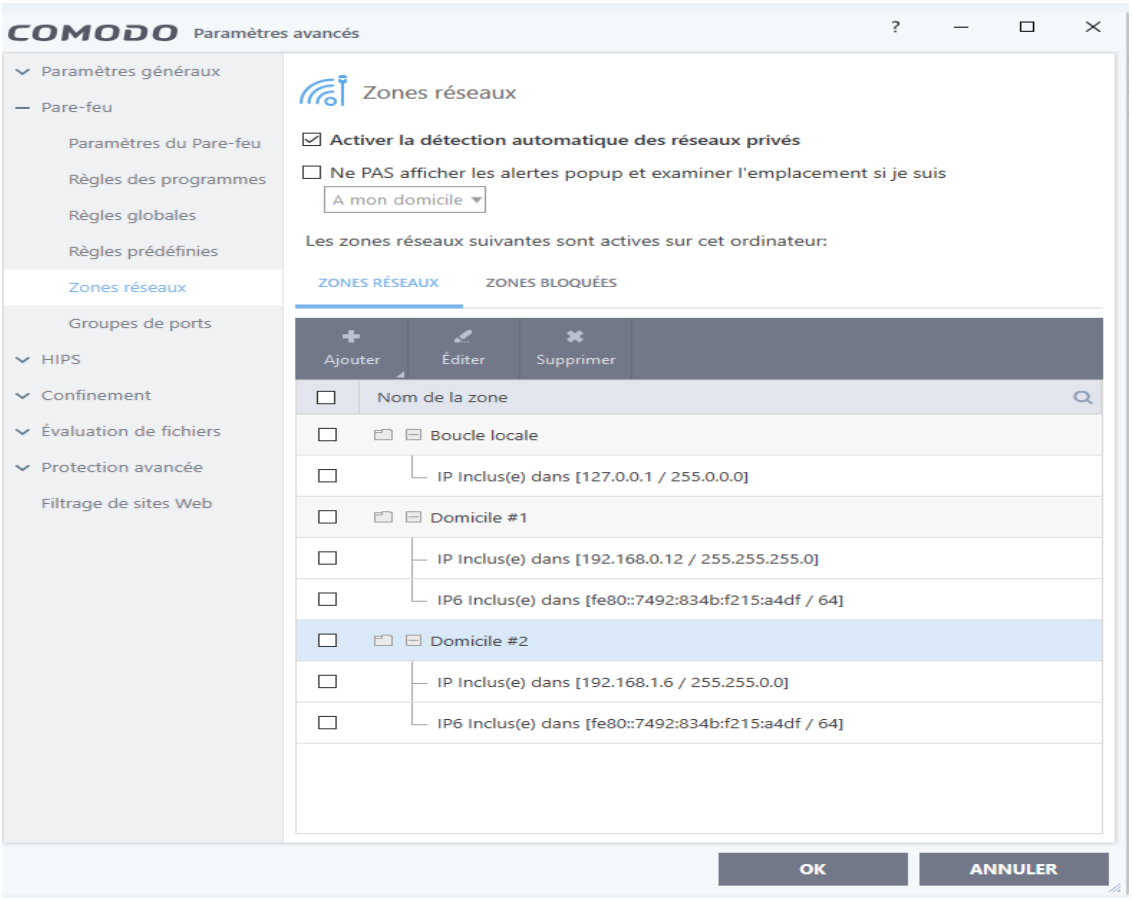
Peu après l'installation de la suite ou du pare-feu, Comodo détecte votre réseau et vous demande de sélectionner votre localisation (cf. fenêtre ci-dessus) :

Si vous cliquez sur « Je suis à mon domicile » cela entraîne la création d'une zone « Domicile #1 » avec mention des plages d'adresses Ipv4 et Ipv6 correspondant à cette zone ainsi que de deux règles globales **d'autorisation** pour ce domicile :

- l'une pour les demandes sortantes si la cible est incluse dans « Domicile #1 »,

- l'autre pour les demandes entrantes si la source est incluse dans « Domicile #1 ».

Si un nouveau réseau est créé ou si vous changez de domicile, Comodo détectera le nouveau réseau et vous adressera une nouvelle demande de localisation : si vous cliquez à nouveau sur **« Je suis à mon domicile »** cela entraînera la création d'une zone « Domicile #2 » avec les plages d'adresses correspondantes, comme dans la fenêtre ci-dessous et de deux nouvelles règles globales **d'autorisation** pour ce nouveau domicile; nous examinerons le rôle de ces règles d'autorisation en étudiant les règles globales (cf. 9.1 et 11.2).



Note : la ou les règles d'autorisation pour les demandes entrantes dont la source est dans Domicile #1 (et #2) devront être transformées en règles de blocage (cf. 9.1.2).

5.3 « Cacher les ports » et bloquer les connexions entrantes venant d'Internet

A partir de la fenêtre d'accueil « Vue avancée » du paragraphe 4, en cliquant sur « Fonctions », **puis** sur « Fonctions du pare-feu », on obtient la fenêtre :

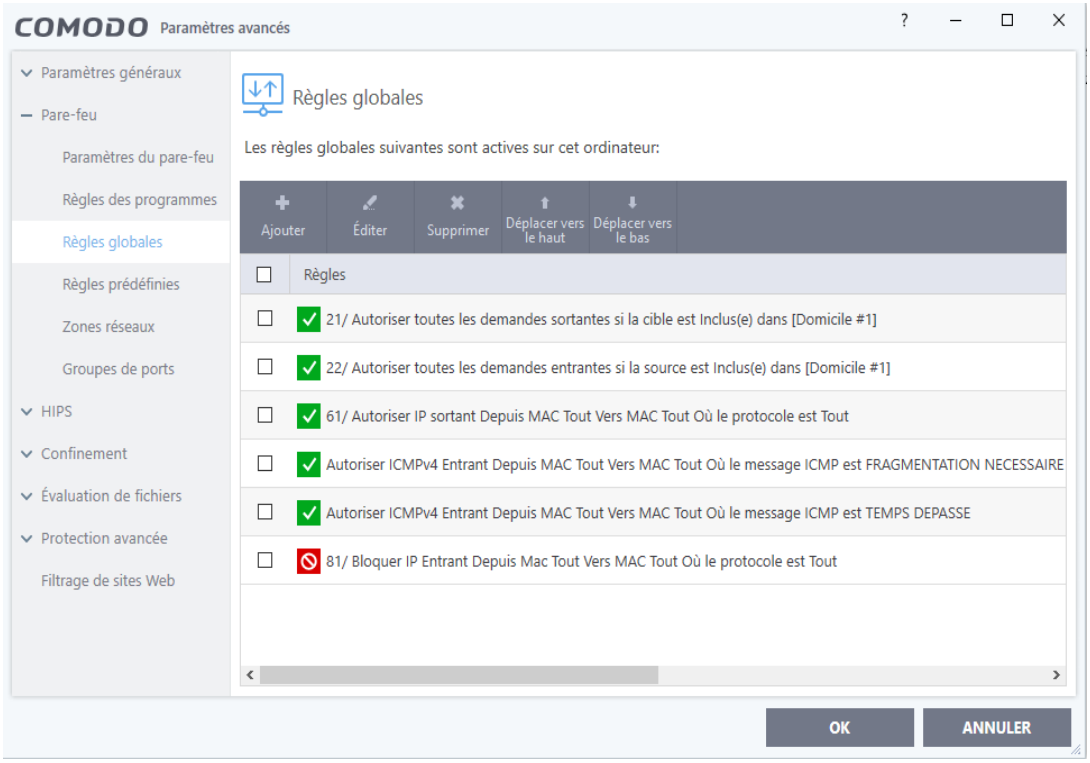
- dans cette nouvelle fenêtre, en cliquant sur « Cacher les ports », **option de configuration la plus importante du pare-feu**, la fenêtre ci-dessous s'ouvre :

Pour davantage de sécurité, il est nécessaire de choisir la première option, « **Bloquer les connexions entrantes** », qui va entraîner, dans la fenêtre des règles globales, la création par Comodo de quatre règles supplémentaires, dont une règle globale « **Bloquer IP entrant** » interdisant les connexions entrantes à partir d'Internet ***et qui rendra votre ordinateur invisible à partir du réseau*** ;

La seconde option, « Alerte sur les connexions entrantes », la 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 ;

Après « Je suis à mon domicile » (cf. 5.2) et « Bloquer les connexions entrantes » la fenêtre des règles globales comporte six règles que nous allons numéroter comme ci-dessous ***(aucune n'est consignée par défaut)*** :



- les deux premières règles, 21/ & 22/, (pour la zone locale au domicile) ont été précédemment obtenues lorsque l'on a choisi la réponse « Je suis à mon domicile » en 5.2 ; il pourrait y avoir des règles identiques pour un éventuel Domicile #2 ;

- la troisième règle, 61/, autorise les demandes de trafic IP sortant vers 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, 81/, bloque pour IP, qui représente 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.

6 Modes de gestion du module pare-feu proposés par Comodo

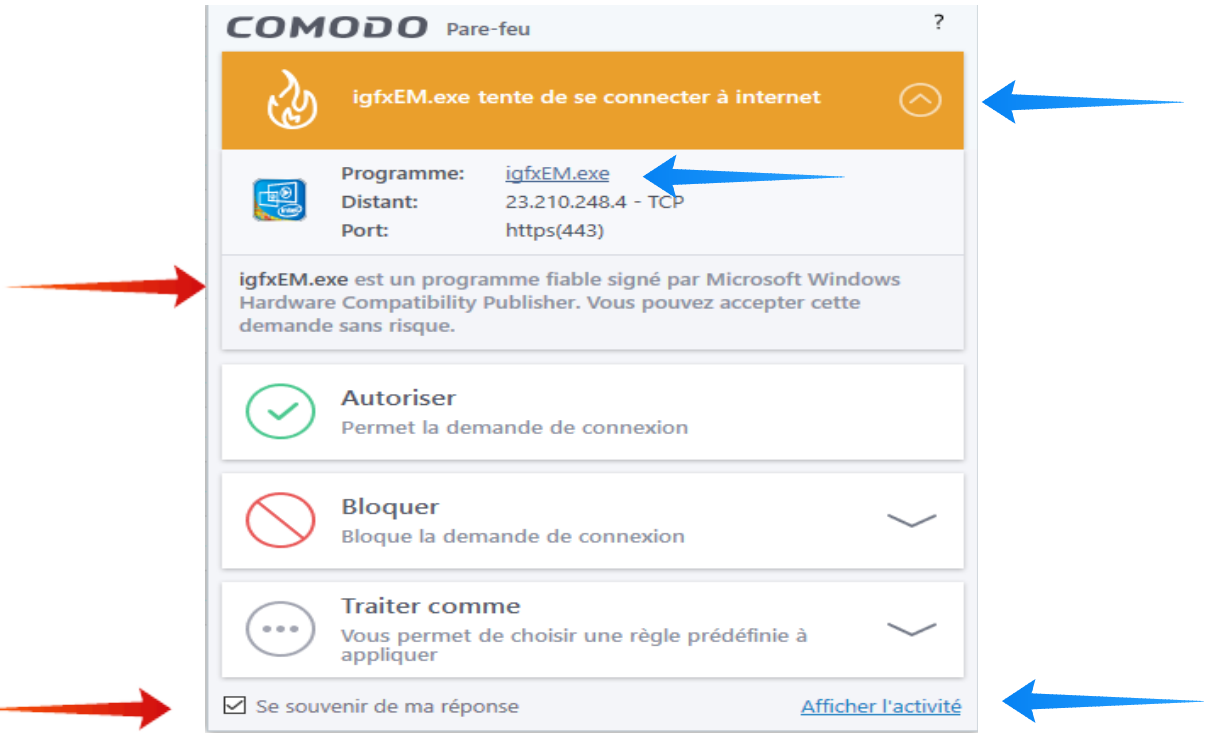
Les différents modes de gestion du pare-feu proposés par Comodo ont été présentés dans le tutoriel précédent (cf. [1] 8.2.2) et sont accessibles à partir de la fenêtre d'accueil **« Vue avancée »** (cf. 4).

La première flèche bleue, la plus à droite de la dite fenêtre « Vue avancée », nous signale le module « Pare-feu » ; un clic gauche déroule un menu qui propose :

6.1 ***« 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 ;

6.2 ***« 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 (voir fenêtre, page suivante) :
- par un bandeau jaune (requête saine), orange (requête de dangerosité imprécise, à évaluer) ou rouge (requête malveillante) ;

- par la mention du programme concerné, de l'adresse distante et du protocole, ainsi que du port concernés ;
- par la mention de la fiabilité de l'application qui demande l'autorisation de connexion : ici « igfxEM est un programme fiable ... », vous pouvez ainsi autoriser cette application, même si vous n'avez pas encore identifié qu'igfxEM correspond à « Intel Graphics Executable Main Module », carte graphique d'Intel : *si le conseil n'apparaît pas, cliquez sur le chevron en haut à droite, dans la barre colorée, pour le déployer ;*
- l'utilisateur peut enfin cliquer sur igfxEM.exe pour obtenir les propriétés de cette application et sur Afficher l'activité qui mentionne le PID, identifiant du processus concerné.

La réponse de l'utilisateur (cf. 8.2) engendrera la création d'une règle sélective et vous ne recevrez plus ultérieurement d'alerte correspondant à cette règle.

L'avantage du mode personnalisé réside dans le fait qu'il offre à l'utilisateur un contrôle complet des règles qui seront appliquées aux demandes de connexion des applications : il sera utilisé pour les niveaux 2 et 3 de sécurité (cf. 10.3).

Par ailleurs les règles prédéfinies, telles que nous les décrivons en 10.1.1 d/, 10.1.1 g/ et 10.1.1 h/ permettent de limiter les alertes à une seule alerte par application, lors de la première requête de celle-ci.

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

- le pare-feu applique 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 lui d'autoriser ou non la demande* : s'il connaît la bonne réputation de cette application et qu'il est en train de l'installer ou de l'utiliser il peut en général l'autoriser ; cependant la demande peut être l'œuvre d'un maliciel : **dans le moindre doute il ne doit pas hésiter 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 malveillant ;

- note* : le nombre d'applications traitées par le Centre Comodo étant de plusieurs

milliers, ces alertes sont rares.

L'avantage du mode sécurisé réside dans son automaticité et dans l'absence presque totale d'alertes.

Le mode dit sécurisé pourra être retenu par ceux qui ne souhaitent pas s'impliquer dans la gestion du pare-feu, ainsi que par les nouveaux utilisateurs qui pourront passer au mode personnalisé, davantage sécurisé, dès qu'ils seront suffisamment familiarisés avec le pare-feu ; ce mode sécurisé sera utilisé pour le niveau 1 de sécurité (cf. 9)

L'inconvénient du mode dit sécurisé réside dans le fait que le niveau de sécurité qu'il assure n'est pas optimal, en effet :

- *toutes les demandes des applications approuvées par Comodo sont autorisées, et cela en direction de tous les ports distants,* ce qui offre des accès potentiels à diverses attaques 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 ;

- si l'utilisateur dispose bien de la possibilité de modifier à posteriori les règles créées par le pare-feu, il ne bénéficie cependant pas, comme dans le mode personnalisé, des alertes et de l'information qu'elles véhiculent, ni de la simultanéité de la demande de connexion avec les logiciels qu'il est en train d'utiliser, ce qui l'éclairerait également sur la nature de la demande ;

= le mode sécurisé est donc paradoxalement moins sûr que le mode personnalisé géré par un utilisateur éclairé par les conseils de Comodo figurant sur les alertes ;

= note : dans le mode 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 5.1), ***ce que nous conseillons*** car cela permet 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).

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

- C**e mode est dangereux,** car le pare-feu crée automatiquement des règles « Autoriser » pour **toutes** les nouvelles demandes et n'envoie aucune alerte !
- Éviter de l'utiliser, 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.

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

7 Quelle politique pour le pare-feu ?

Nous présentons ici trois niveaux de sécurité croissante, les niveaux 2 et 3 supposant que le précédent niveau ait été mis en place : en effet le pare-feu Comodo étant suffisamment souple permet d'évoluer progressivement vers une gestion rigoureuse du pare-feu qui, idéalement, n'autoriserait que les applications qui vous sont nécessaires et n'ouvrirait que les ports indispensables.

- **le Niveau 1 de sécurité** (cf. 9) constitue la première étape de cette démarche. Il assure déjà 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 celle du pare-feu Windows. Il consiste à bloquer la totalité des connexions entrantes, ainsi que les processus d'administration et services les plus dangereux ; il nécessite une demi-heure environ de paramétrage initial, avec choix de la gestion du pare-feu **en mode sécurisé** : le pare-feu autorisera automatiquement **toutes les demandes de connexions des applications jugées saines par le Centre Comodo** avec seulement de rares alertes pour les demandes des autres applications ; si vous retenez ce mode vous pouvez passer directement au paragraphe 9 après avoir jeté un coup d'œil sur le paragraphe 8 ;

- **le Niveau 2 de sécurité** (cf. 10) assure un niveau de sécurité nettement accru ; 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 auront été élaborées ;

- **le Niveau 3 de sécurité** (cf. 11) est destiné à l'utilisateur expérimenté, ayant déjà

mis en place le niveau 2 de sécurité, et désirant exercer **un contrôle étroit du trafic** ; il lui permet, grâce à l'emploi des règles globales, de contrôler toutes les connexions entrantes et sortantes de son ordinateur avec Internet et son réseau local (imprimante, télévision et autres objets connectés) et assure ainsi une sécurité optimale.

8 La gestion des alertes et les outils généraux de gestion des règles

8.1 Niveau de fréquence des alertes passé de « Bas » à « Haut »

C**oncernant le niveau de fréquence d'alerte passé de « Bas » à « Haut »** (cf. 5.1 b/), il faut signaler que 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 ;

et précisons, **à titre didactique pour ceux qui désirent évoluer vers les niveaux 2 et 3 de sécurité**, que pour une réponse « Autoriser » à l'alerte du paragraphe 6.2 :

- le niveau **très bas** n'engendrera qu'une règle par application, ici : *« Autoriser IP **entrant-sortant** depuis Mac Tout vers MAC Tout où le protocole est Tout »,* ceci est extrêmement dangereux et doit être proscrit ;

- le niveau **bas** engendrera une règle d'autorisation pour la totalité du trafic **IP sortant:** *« Autoriser IP **sortant** depuis Mac Tout vers MAC Tout où le protocole est Tout »,* ceci est peu restrictif *;*

- le niveau **moyen** engendrera une ou deux règles plus sélectives, **par protocole** (**TCP** ou **UDP),** par exemple ici **:** *« Autoriser TCP sortant depuis MAC Tout vers MAC Tout où le port source est Tout et **le port de destination est Tout** »*

- le niveau **haut** engendrera des règles plus sélectives, **par protocole et par port ;** ainsi, ici, deux règles, l'une pour le port 80 : « *Autoriser TCP sortant de MAC Tout vers MAC Tout où le port source est Tout et **le port de destination est 80** » **et l'autre pour le port 443** ;*

- le niveau **très haut** engendrera des règles **par protocole, port et adresse ;** soit une ou deux règles par adresse, les adresses pouvant être multiples ; ainsi pour l'une d'entre elles, correspondant à l'alerte du paragraphe 6 on aura : « *Autoriser TCP sortant depuis MAC Tout vers IP 23.210.248.4 où le port source est Tout et le port de destination est 443*» ;

Aussi évitera-t-on 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 à la fois 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, et si vous êtes en mode personnalisé, l'utilisation des règles prédéfinies explicitées au paragraphe 10.1 vous permettra de n'avoir en général qu'une seule alerte par application lors de la première demande de celle-ci.

8.2 Gestion des alertes du pare-feu

Afin de pouvoir bénéficier de façon optimale des alertes, du pare-feu il est nécessaire dans « Paramètres du par-feu » (cf. 4) :
- de décocher « Ne pas afficher les alertes popup » ;
- de cocher « Activer les alertes Trustconnect » ;
- de cocher « Niveau de fréquence d'alerte **Haut » (et non Bas)** ;
- d'accroître éventuellement la durée d'alerte à l'écran, par exemple de 100 à 300 s.

Les réponses que l'on fait alors à ces alertes engendrent **la création de règles sélectives par application, protocole et port (cf. 8.1.) et vous ne recevrez plus, ultérieurement d'alertes correspondant à ces règles pour cette application.**

L'alerte (voir la fenêtre de la page suivante) informe l'utilisateur :

- par un bandeau jaune (requête saine), orange (requête de dangerosité imprécise, à évaluer) ou rouge (requête malveillante) ;

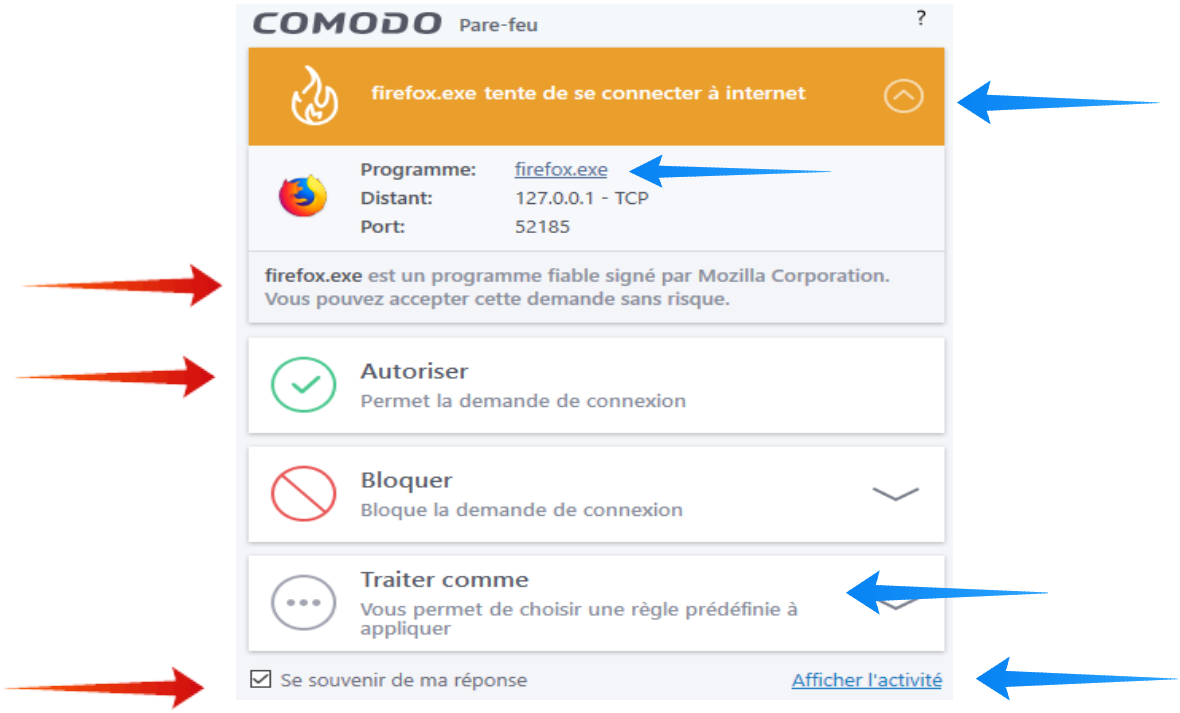
- par la mention du programme concerné, de l'adresse distante et du protocole, ainsi que du port concernés ;

- par une mention de la fiabilité du programme qui demande l'autorisation de connexion, ici : « firefox est un programme fiable signé par Mozilla Corporation. Vous pouvez accepter cette demande sans risque. » (Comodo a évalué la fiabilité de milliers de programmes) : *si le conseil n'apparaît pas, cliquez sur le chevron en haut à droite, dans la barre colorée, pour le déployer ;*

- enfin l'utilisateur peut, s'il le désire :

a/ cliquer sur firefox.exe pour consulter les propriétés de cette application ;

b/ cliquer sur Afficher l'activité qui mentionne le PID, identifiant du processus concerné.



Quel choix pour vos réponses ?

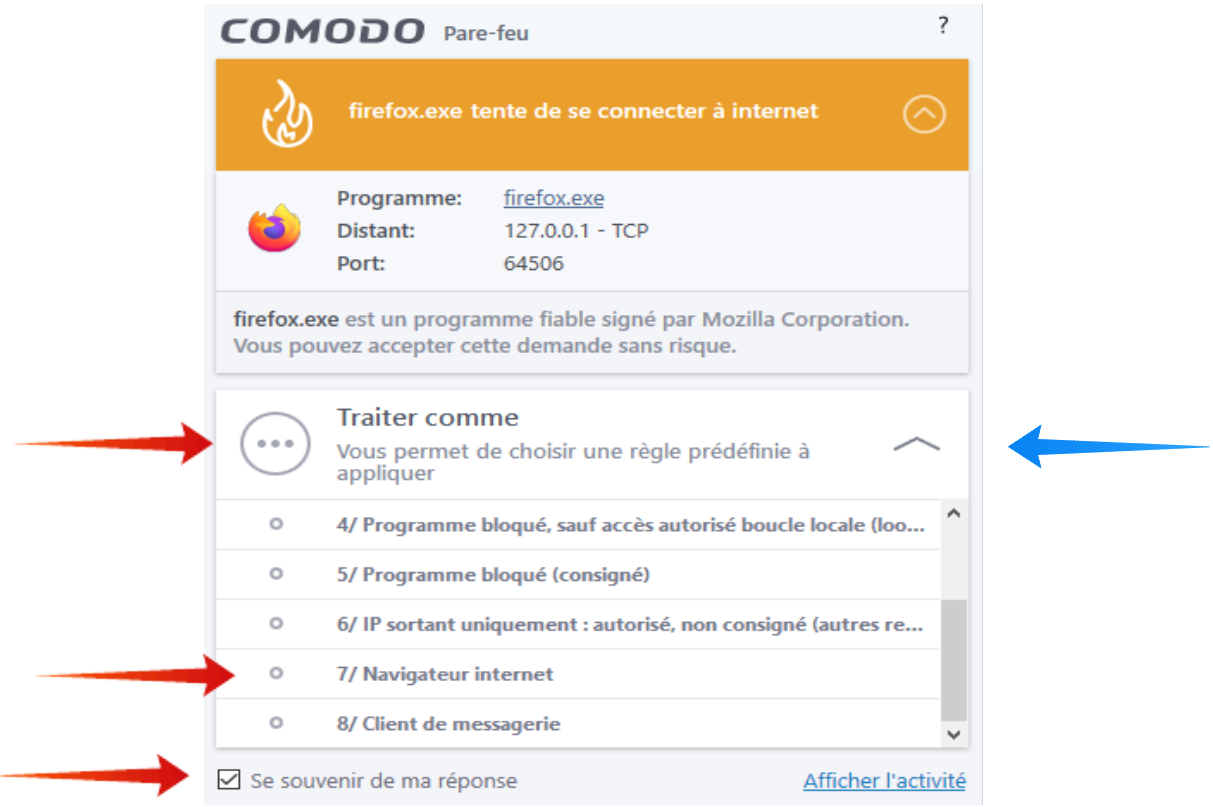
- a/ **« Autoriser » pour cette seule demande** en décochant « Se souvenir de ma réponse » (par exemple lors d'un téléchargement) ;

- b/ **ou de façon permanente** en cochant « Se souvenir de ma réponse » (par exemple pour les applications Windows ou vos applications courantes), cette autorisation n'étant valable qu'en direction du seul port mentionné dans la demande ;

- c/ mais pour les applications non Windows qui font souvent successivement de multiples demandes de connexions en direction de plusieurs ports distants, **il est bien préférable de cliquer sur le chevron « Traiter comme »** afin de déployer le menu des règles prédéfinies que nous compléterons en 10.1 et de choisir, après avoir coché *« Se souvenir de ma réponse »,* la règle prédéfinie la plus appropriée :
- *Navigateur internet* (dans le cas présent pour le navigateur Firefox) ;
- *Client de messagerie ;*
- *Application limitée autorisée (*obtenue à partir de la règle par défaut « **Application autorisée** » en en restreignant le champs d'autorisation pour des raisons de sécurité : cf . 10.1.1 d/).

Le grand intérêt de ces règles prédéfinies réside dans le fait de délivrer en une seule fois l'ensemble des autorisations ou blocages de connexions que pourrait

solliciter une application et d'éviter ainsi une multitude d'alertes (cf. 10.1) :

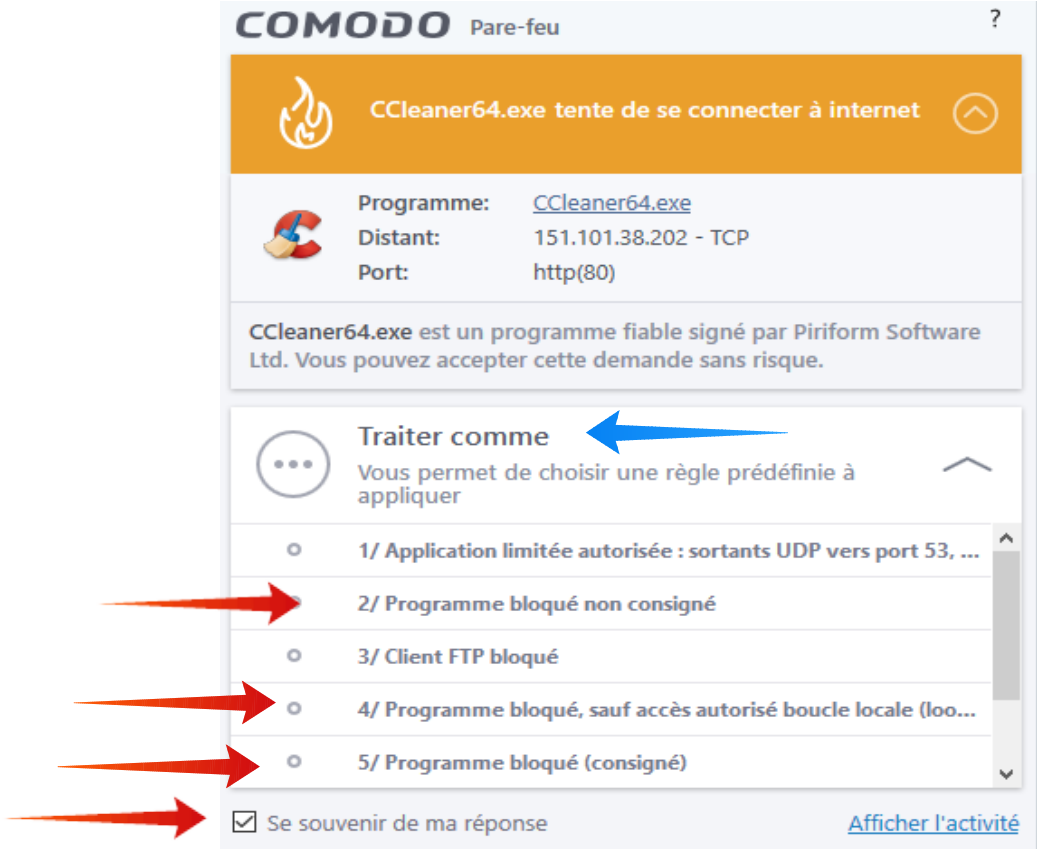


- d/ « Bloquer » : si Viruscope est activé (cf. tutoriel précédent [1]) et que vous cliquez
sur « Bloquer », les trois options ci-dessous se déploient pour s'offrir à votre choix :

- *Bloquer uniquement ;*
- *Bloquer et interrompre* (avec interruption du processus demandeur) ;
- *Bloquer, interrompre et rétroaction* (avec interruption du processus demandeur et annulation des modifications apportées par le processus à d'autres processus) ;

- pour une alerte exceptionnelle de demande de connexion d'un cheval de Troie (Trojan), on choisira sans hésiter **« Bloquer, interrompre et rétroaction »** ;

- e/ dans les autres cas où l'on désire bloquer une demande il est préférable de choisir parmi les règles prédéfinies 2/, 4/ ou 5/ ci-dessous :



= « **2/ Programme bloqué non consigné** » si l'on ne désire pas utiliser l'application (par exemple, pour des raisons de confidentialité, Cortana), et que l'on ne désire pas encombrer le journal ;

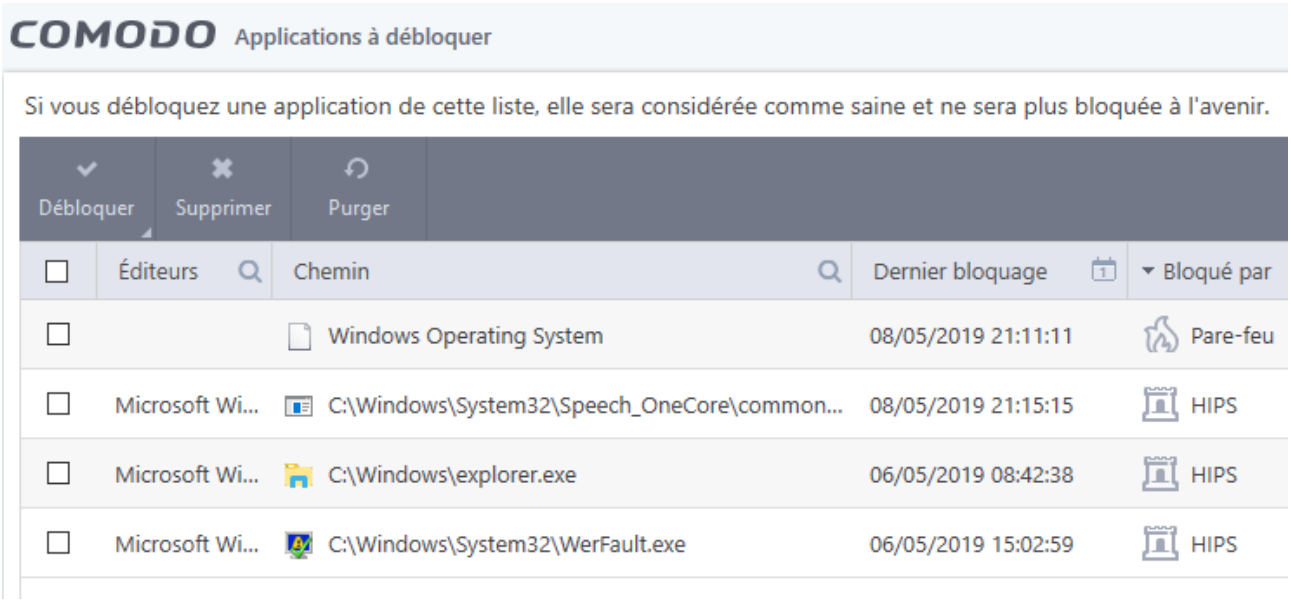
= « **4/ Programme bloqué, sauf accès à la boucle locale (loopback)** », pour une application que l'on utilise, dont l'accès à la boucle locale est nécessaire à son bon fonctionnement, mais dont on ne souhaite pas qu'elle accède à Internet ; comme pour le bon logiciel de nettoyage C-Cleaner ci-dessus ou pour un logiciel de photos ;

= « **5/ Programme bloqué (consigné)** » pour suivre les requêtes bloquées d'une application dont on désire suivre l'activité.

Cas particulier : attention de 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 » serait créée et se substituerait à

la règle « Demander ».

8.3 Gestion des « Applications bloquées »



A suivre en cours d'utilisation afin de débloquer d'éventuelles applications indispensables (antivirus, etc.) :

mais, **Attention,** l'*appellation « Applications bloquées » est trompeuse : en mode personnalisé, il s'agit plutôt d'un journal des alertes pare-feu et HIPS soumises à l'utilisateur, car, que sa réponse soit « Bloquer » ou même « Autoriser », l'application est mentionnée dans cette fenêtre.*

a/ le chemin de l'application est suivi de la date et de l'heure du dernier blocage et du module responsable du blocage ce qui permet de la repérer soit dans le « Journal événements pare-feu » (ou plus directement dans « Intrusions réseaux »), soit dans « Journal événements HIPS » où la nature et le détail de l'action concernée sont précisés ;

b/ un clic droit sur l'application concernée permet :
- en 1ère ligne, de débloquer un ou tous les composants de sécurité du blocage ;
- en 2ème ligne de consulter les détails du fichier concerné et de son évaluation ;
- en 3ème ligne, d'ôter (remove) l'application de la liste *(et non de supprimer le blocage comme pourrait le faire croire la traduction approximative)* ;
- en 4ème ligne de purger la liste des applications qui ne sont plus en activité.

c/ pour une application figurant dans ce tableau on peut :

- ne rien faire ;

- ou, en 3ème ligne, cliquer sur **« Supprimer »**, ce qui ôtera l'application de la liste, et laissera, dans le tableau des règles de programmes ou dans celui des règles HIPS, toute règle engendrée par une éventuelle réponse antérieure de votre part à une alerte ;

- ou, en 1ère ligne, **« Débloquer »** pour un composant de sécurité, mais attention cela remplace la règle que vous aviez précédemment choisie lors d'une réponse à une alerte par la règle « Application autorisée » qui accorde malencontreusement à cette application ***:***
= pour une règle de programmes, les droits les plus étendus aussi bien en entrée qu'en sortie ; il importe donc de modifier aussitôt, dans le tableau des règles de programmes, cette nouvelle règle en fonction de la nature de la demande signalée en a/ et de l'objectif poursuivi : vous pouvez par exemple, choisir une des règles prédéfinies d'autorisation (limitée) ou de blocage que nous allons mettre en place au paragraphe 10.1 des règles prédéfinies ; **n'hésitez pas à bloquer systématiquement les connexions entrantes pour les applications ;**
= et, pour une règle HIPS, tous les droits d'accès (à l'exception de Demander pour lancer un exécutable exe.), règle d'autorisation que vous pouvez modifier en « Programme limité » ou « Programme confiné » (cf. [2] General Tasks\Introduction\Manage Blocked Items).

8.4 Les « Journaux » [accessibles à partir de Vue avancée (4)]

Les journaux de la suite et du pare-feu Comodo sont nombreux et particulièrement bien conçus ; parmi eux, le journal « Evènements Pare-feu » est indispensable pour surveiller le trafic et gérer les règles (cf. 11.1 et 11.2).

8.4.1 Paramètres généraux : « Journaux » : cf. tutoriel d'installation ([1] 10.1.3).

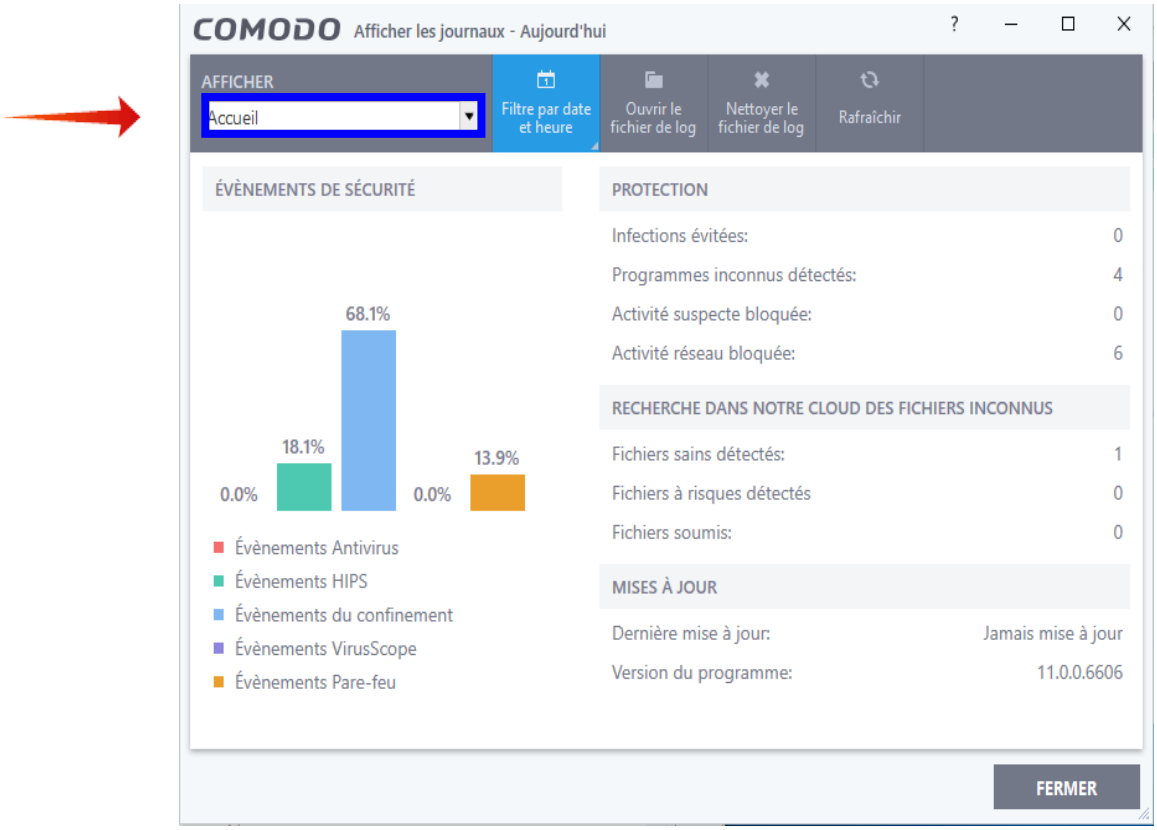
8.4.2 Optimisation du journal « Événements Pare-feu »

Par le jeu du choix et du positionnement des règles globales, ainsi que de la consignation ou non des règles de programmes, et surtout des règles globales, l'utilisateur veillera à ne pas encombrer inutilement ce journal et ainsi à le rendre aisément consultable.

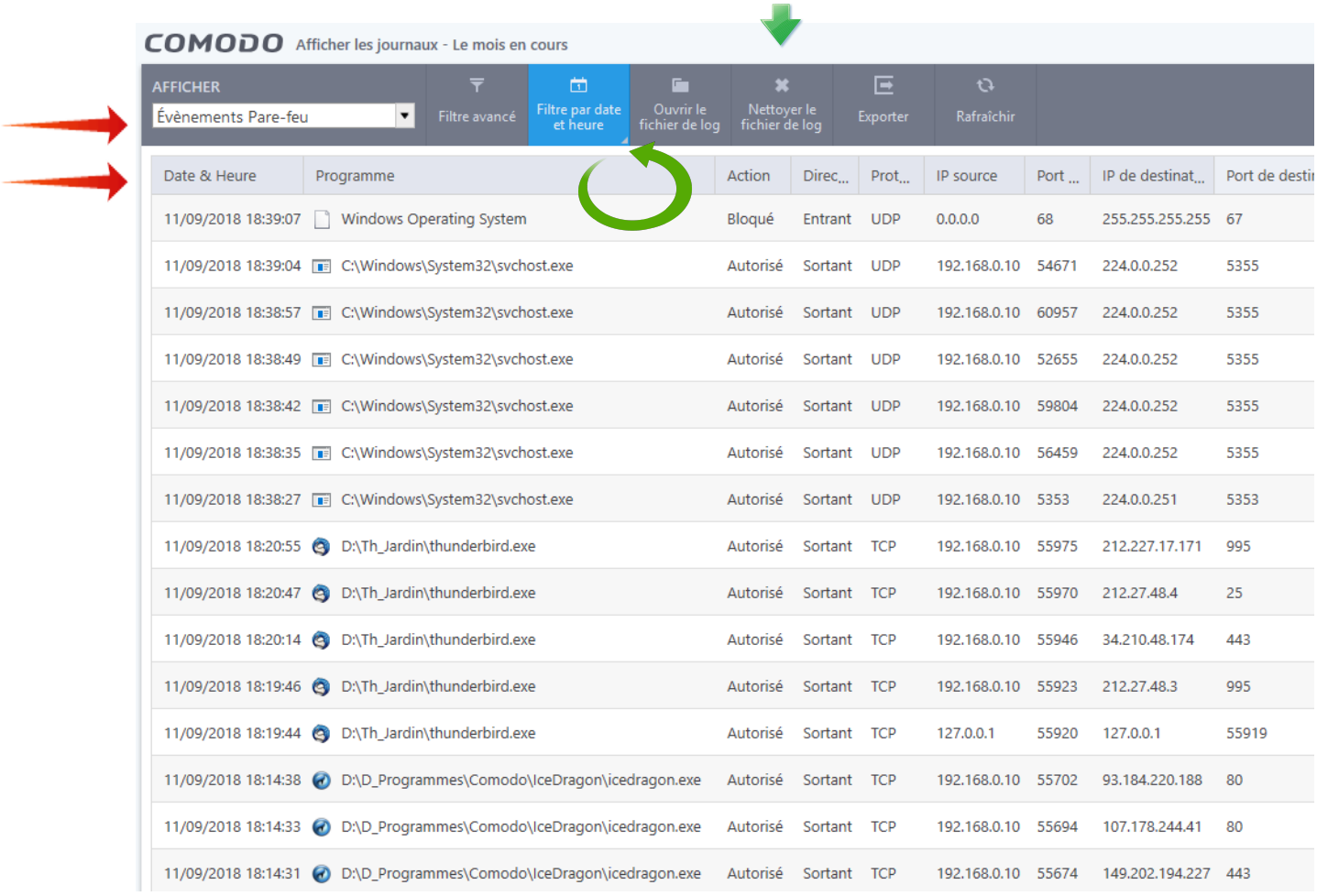
Ainsi la case « consigné » des règles globales et de programmes permet :
- si elle est cochée de répertorier dans le Journal des Événements les demandes de connexions, et ainsi :
= de s'assurer qu'une règle a été correctement configurée pour l'utilisation ou l'installation d'un programme, d'une imprimante et, si nécessaire, de décider de la modifier ;
= de repérer les connexions abusives ou, moins fréquemment, d'éventuelles attaques de pirates.
- si elle est décochée, de ne pas encombrer inutilement le Journal des Événements et ainsi de surveiller plus aisément le trafic restant (cf. fin de 9.2 en italiques).

8.4.3 Utilisation du journal « Événements Pare-feu »

A partir de la fenêtre « Vue avancée », en 4, l'accès le plus rapide au journal se fait en cliquant sur l'onglet **« Intrusions réseau »** ou à partir de l'onglet **« Journaux »**, puis dans la fenêtre ci-dessous qui s'ouvre, d'« Événements Pare-feu » dans le menu déroulant du cadre « Accueil » , en haut, à gauche ;



- dans les deux cas s'ouvre alors la fenêtre page suivante) du journal « **Événements Pare-feu** » où l'on évitera de nettoyer le fichier des logs ce qui remettrait à zéro l'ensemble des journaux ; par contre en cliquant sur la petite flèche en bas à droite de l'onglet « Filtre par date et heure », on aura un grand choix pour sélectionner la période que vous désirez, depuis « moins de 1 h », à une période entre deux dates pouvant atteindre plusieurs mois.

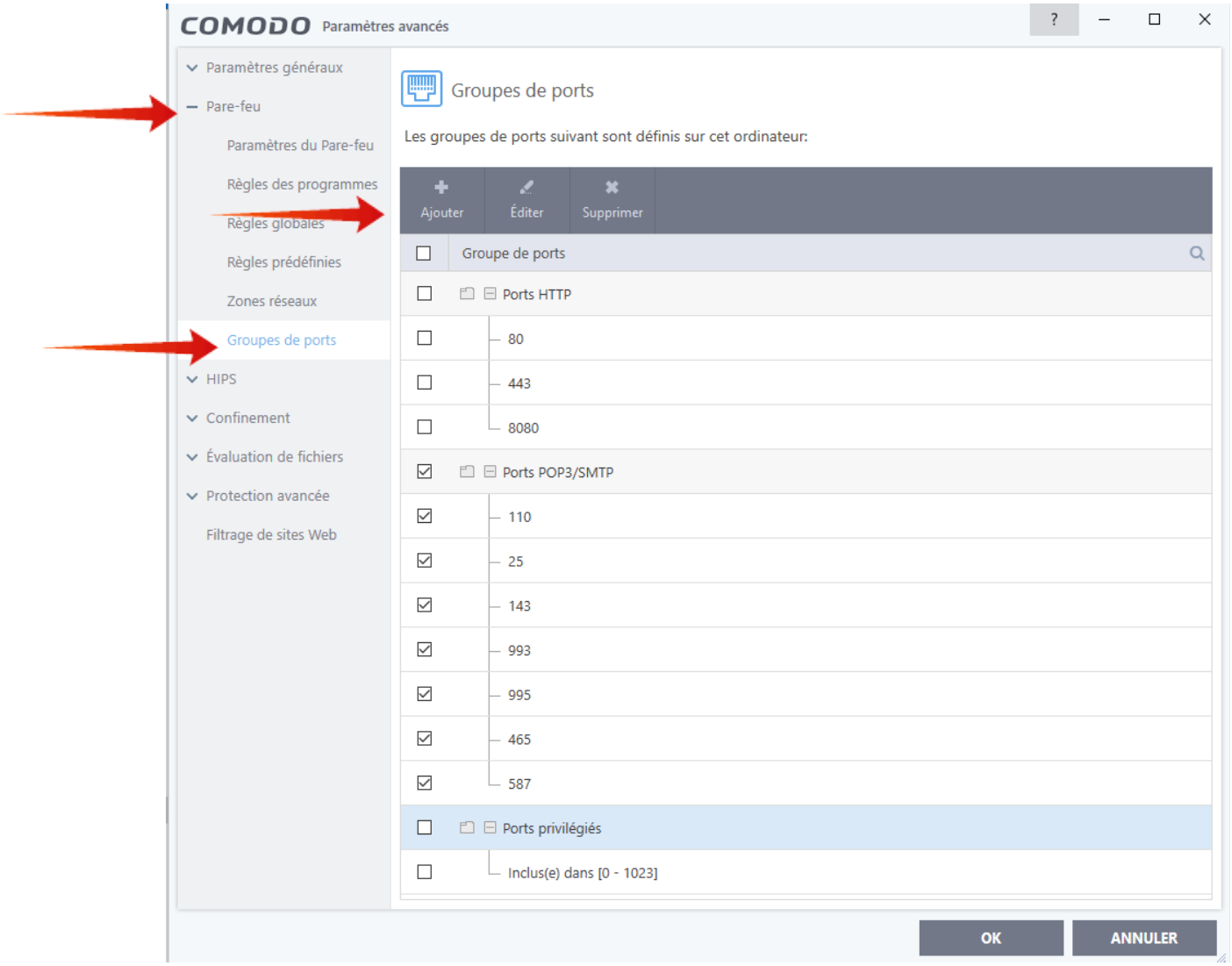


Date & Heure	Programme	Action	Direc...	Prot...	IP source	Port ...	IP de destinat...	Port de desti
11/09/2018 18:39:07	Windows Operating System	Bloqué	Entrant	UDP	0.0.0.0	68	255.255.255.255	67
11/09/2018 18:39:04	C:\Windows\System32\svchost.exe	Autorisé	Sortant	UDP	192.168.0.10	54671	224.0.0.252	5355
11/09/2018 18:38:57	C:\Windows\System32\svchost.exe	Autorisé	Sortant	UDP	192.168.0.10	60957	224.0.0.252	5355
11/09/2018 18:38:49	C:\Windows\System32\svchost.exe	Autorisé	Sortant	UDP	192.168.0.10	52655	224.0.0.252	5355
11/09/2018 18:38:42	C:\Windows\System32\svchost.exe	Autorisé	Sortant	UDP	192.168.0.10	59804	224.0.0.252	5355
11/09/2018 18:38:35	C:\Windows\System32\svchost.exe	Autorisé	Sortant	UDP	192.168.0.10	56459	224.0.0.252	5355
11/09/2018 18:38:27	C:\Windows\System32\svchost.exe	Autorisé	Sortant	UDP	192.168.0.10	5353	224.0.0.251	5353
11/09/2018 18:20:55	D:\Th_Jardin\thunderbird.exe	Autorisé	Sortant	TCP	192.168.0.10	55975	212.227.17.171	995
11/09/2018 18:20:47	D:\Th_Jardin\thunderbird.exe	Autorisé	Sortant	TCP	192.168.0.10	55970	212.27.48.4	25
11/09/2018 18:20:14	D:\Th_Jardin\thunderbird.exe	Autorisé	Sortant	TCP	192.168.0.10	55946	34.210.48.174	443
11/09/2018 18:19:46	D:\Th_Jardin\thunderbird.exe	Autorisé	Sortant	TCP	192.168.0.10	55923	212.27.48.3	995
11/09/2018 18:19:44	D:\Th_Jardin\thunderbird.exe	Autorisé	Sortant	TCP	127.0.0.1	55920	127.0.0.1	55919
11/09/2018 18:14:38	D:\D_Programmes\Comodo\IceDragon\icedragon.exe	Autorisé	Sortant	TCP	192.168.0.10	55702	93.184.220.188	80
11/09/2018 18:14:33	D:\D_Programmes\Comodo\IceDragon\icedragon.exe	Autorisé	Sortant	TCP	192.168.0.10	55694	107.178.244.41	80
11/09/2018 18:14:31	D:\D_Programmes\Comodo\IceDragon\icedragon.exe	Autorisé	Sortant	TCP	192.168.0.10	55674	149.202.194.227	443

Dans le tableau ci-dessus on peut observer :
- en première date, une demande entrante de Windows Operating System, du port 68 vers le port 67 (DHCP), bloquée, comme toutes les connexions entrantes ;
- puis des demandes autorisées de svchost.exe vers les ports 5353 et 5555 (bloquées ultérieurement car non indispensables pour notre imprimante HP de la série 4650) ;
- des demandes autorisées du Client de messagerie Thunderbird vers le port SMTP 25 (remplacé depuis par le port 465), le port POP3 sécurisé 995 et le port HTTPS 443 ;
- des demandes du navigateur IceDragon de Comodo vers les ports HTTP 80 et HTTPS 443.

Par défaut les événements sont classées par ordre décroissant de date et d'heure ; en cliquant sur l'en-tête de chaque colonne vous obtenez des classements différents :
- le classement par IP source vous permet d'analyser l'implication de chaque machine connectée, pourvu que vous ayez programmé des adresses IP fixes dans la box (cf. 1.4.7 e/ et Annexe A - Centre Réseau et partage A.1 Désactiver DHCP) ;
- le classement par ports de destination est particulièrement précieux, notamment pour élaborer les règles globales ;
- une dernière colonne « Alerte » signale les alertes liées que l'on peut consulter d'un clic.

8.5 Les « Groupes de ports »



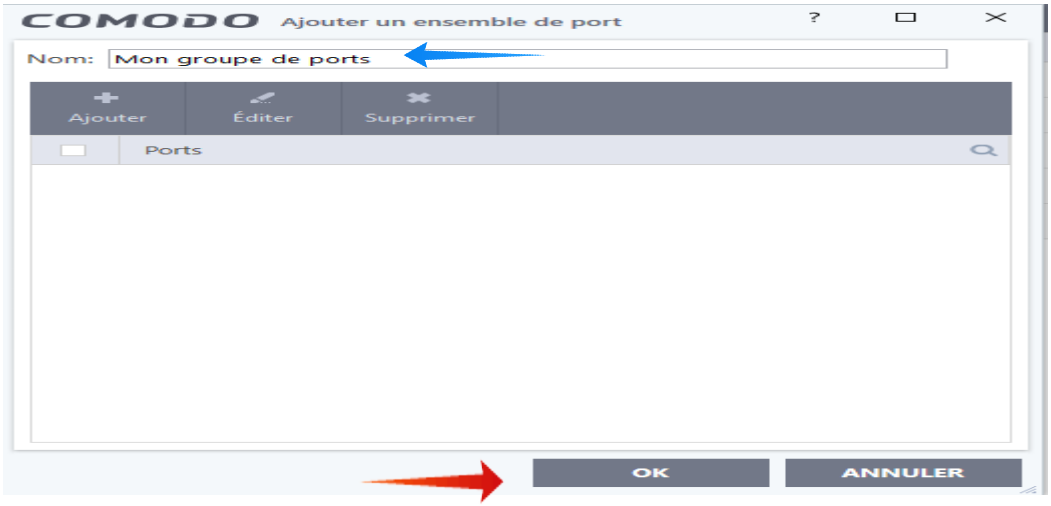
Afin de paramétrer les groupes de ports, cliquez sur l'onglet « Paramètres » de l'une des fenêtres d'accueil, puis, dans la fenêtre de la page précédente, sur l'onglet « Pare-feu », enfin sur l'onglet « Groupes de ports ». Ceux-ci sont utilisés lors de la création de certaines règles globales ou de programmes. Par défaut sont programmés les groupes de ports de cette fenêtre de la page précédente :

- Le **groupe de ports HTTP** sera utilisé par les navigateurs, le client de messagerie et de nombreuses règles ; les ports HTTP, utilisés par les serveurs Web, comprennent les ports 80 (HTTP) et 443 (HTTPS, version sécurisée de HTTP), ainsi que le port 8080, port 8080 ne nécessitant pas des privilèges d'administrateur « root » (lequel possède toutes les permissions sur le système) et utilisé par des proxy ainsi que par des pirates pour usurper l'identité d'un PC et en pirater d'autres.

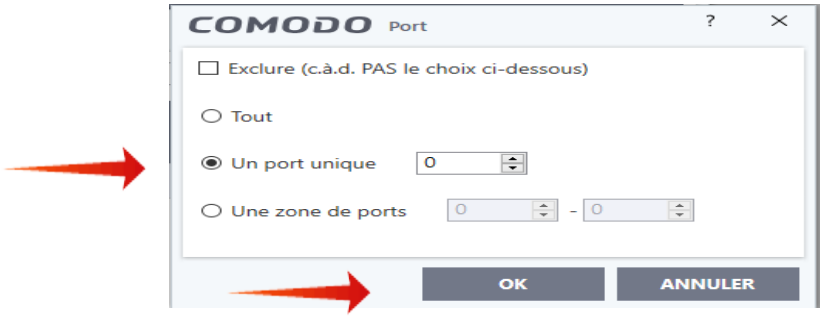
- **Le groupe des ports POP3 et SMTP** est utilisé par les clients de messagerie tels Thunderbird ou Outlook (les clients de messagerie permettent de stocker les courriels sur son ordinateur, au lieu de le laisser sur les sites des serveurs de messagerie des fournisseurs d'accès Internet).

- **Le groupe des ports privilégiés** (de 0 à 1023) est utilisé par la sous-règle « Autoriser les requêtes FTP passives sortantes » faisant partie de la règle prédéfinie Client FTP (cf. 10.1.1 c/) ; les ports intitulés « privilégiés » par Comodo sont les ports « bien connus », de 0 à 1023, signalés en 1.1 ;

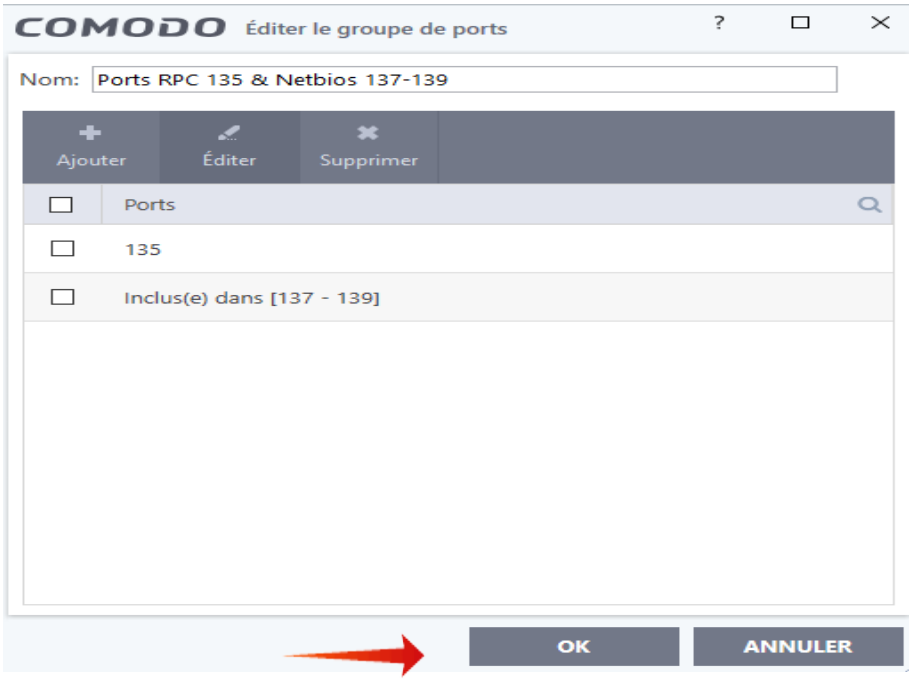
A titre d'exemple nous allons ajouter le groupe de ports Netbios qui nous permettra de bloquer ce système fort dangereux (cf . 1.4.7 f) :
- dans la fenêtre précédente cliquer sur « Ajouter » : on obtient la fenêtre ci-dessous :



- remplacer l'intitulé « Mon groupe de ports » par le nouvel intitulé, ici **« Ports RPC 135 et Netbios 137-139» ;**
- cliquer sur l'onglet « Ajouter » pour obtenir la fenêtre suivante où l'on ajoutera successivement les ports envisagés, soit le port 135 dans l'encadré « Un port unique » et les ports 137 à 139 dans l'encadré « Une zone de ports » ;



- faire OK en bas de chacune des fenêtres successivement ouvertes :
- on obtient finalement :



Attention, ne supprimez pas un groupe de ports, cela pourrait entraîner des décalages de ports d'un groupe à l'autre se répercutant au niveau des règles les utilisant. Et ne supprimez pas un port sur un groupe déjà constitué : ce groupe de ports pourrait se révéler inefficient. Par contre vous pouvez ajouter à la queue leu leu autant de groupes de ports que vous le désirez .

9 Niveau 1 de sécurité - Sécurisation minimale essentielle

Ce niveau complète la configuration de base décrite en [1] et reprise en *5.1 : Configuration des paramètres du pare-feu* et en *5.3 : « Cacher les ports » et bloquer les connexions entrantes provenant d'Internet* ; ce complément de sécurisation consiste :

- à bloquer les demandes entrantes originaires de la zone locale (Domicile # 1) ;

- à créer des règles globales de blocage concernant les connexions des protocoles dangereux ICMPv4, ICMPv6, IGMP et des processus SMB, Netbios, SSDP et SNMP qui pourraient faciliter les intrusions de pirates, règles globales que nous placerons au dessus des règles 21/ et 22/ concernant le domicile.

Avec ce niveau de sécurisation de base on bénéficiera du fait que :
- les ports sont cachés et toutes les connexions entrantes, y compris de la zone locale, sont bloquées ;
- les demandes des protocoles dangereux, ci-dessus mentionnés, sont bloquées, ;
- les règles pour les demandes de connexions sortantes, ne seront créées automatiquement que pour les applications jugées saines par Comodo.

Les inconvénients de ce niveau de sécurité sont ceux du mode sécurisé : vous ne contrôlez pas les connexions sortantes ; toutes les applications considérées comme saines par Comodo sont autorisées à se connecter à Internet, avec les risques éventuels que cela peut comporter (cf. 6.3).

Si vous désirez davantage de sécurité et contrôler plus étroitement le trafic concernant votre ordinateur vous pourrez passer au niveau 2 lorsque vous vous serez suffisamment familiarisé avec le pare-feu.

9.1 Blocage des connexions entrantes

9.1.1 Blocage des connexions entrantes en provenance d'Internet

Ce blocage constitue la précaution de sécurité la plus importante du pare-feu : il a été obtenu par le choix, décrit en 5.3, de l'option « Cacher les ports », puis de « Bloquer les connexions entrantes » (en provenance d'Internet) qui a engendré la règle globale « Bloquer IP entrant ... » (non consigné) ; cela est à faire sans tarder si cela n'a déjà été fait.

Même pour des applications saines les connexions entrantes en provenance d'Internet doivent, autant que possible, être évitées ; lorsqu'une telle connexion est indispensable, par exemple pour une assistance à distance avec une personne de toute confiance ou pour un jeu, la règle devra être aussi restrictive que possible avec mentions du protocole, des adresses source et de destination, 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).

9.1.2 Blocage des demandes entrantes provenant de la zone locale (Domicile # 1)

Dans le tableau des Règles globales (cf. 5.3) il est important de transformer *la règle « 22/ Autoriser toutes les demandes entrantes si la source est incluse dans Domicile #1 »* en règle de blocage **consignée** ; pour ce faire cliquer sur cette règle puis faire « Editer », et choisir « Bloquer » au lieu d' « Autoriser » et **cocher la case « Consigner ... »**, on obtient la règle de blocage appropriée, que l'on a numérotée 22/, dans le tableau situé en 9.2. Jointe à la règle 81/, cette règle bloquera toutes les demandes de connexions entrantes, dont celles des services dangereux (on opérerait de même pour une éventuelle zone locale Domicile #2).

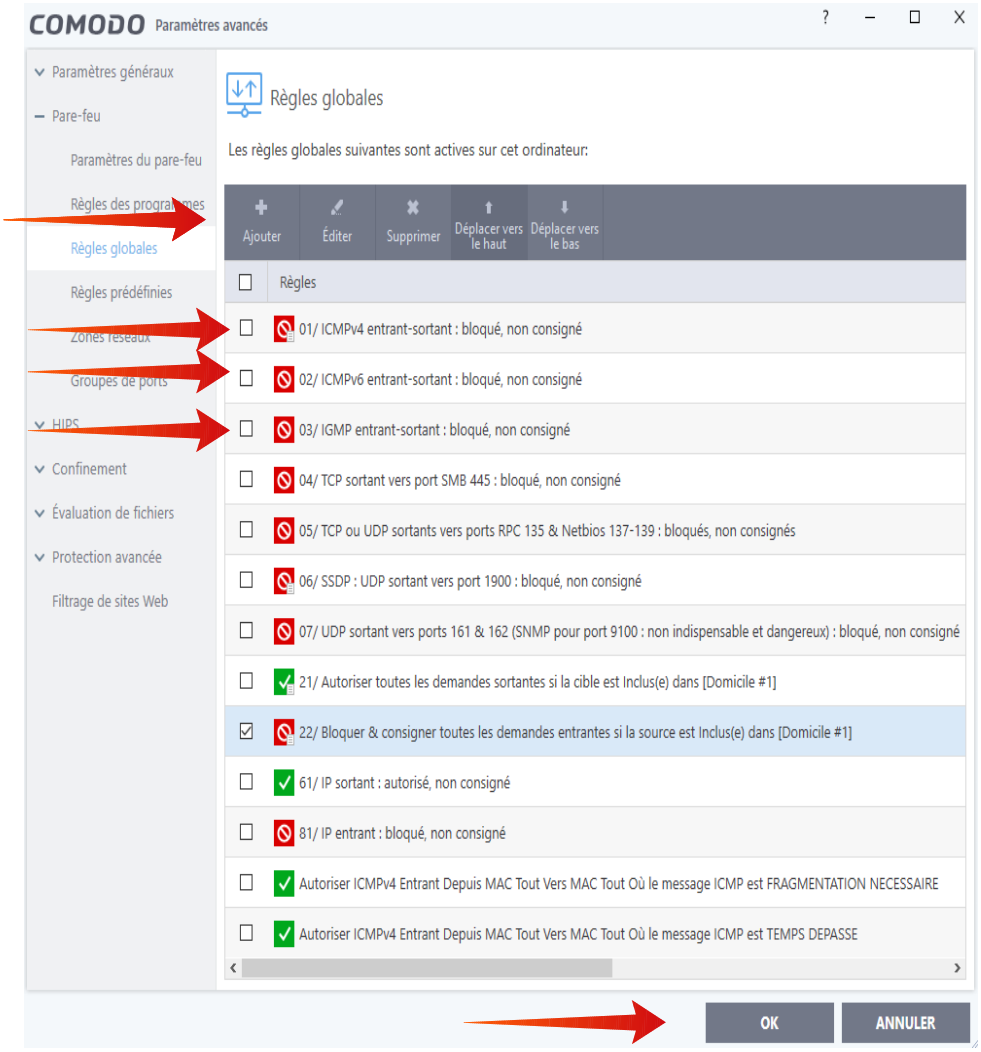
Cette règle 22/ étant consignée, apparaîtront dans le tableau « Intrusions Réseau » (et dans le Journal des événements pare-feu) la liste des demandes de connexions entrantes bloquées, certaines provenant
- de votre imprimante (enregistrées de 11/ à 13/ dans le tableau du paragraphe 13 que l'on consultera) et de DHCP, (ce qui *ne devrait pas vous empêcher d'accéder à Internet ou à votre imprimante : vérifiez-le) ;*
- des objets connectés du réseau local, ce qui est l'un des objectifs recherchés, car il n'est pas souhaitable de connecter directement ceux-ci sur l'ordinateur principal (cf. 1.6) ;
- d'ICMP et d'IGMP pour lesquels nous allons créer ci-dessous des règles spécifiques, non consignées, et que nous placerons en tête du tableau afin que les demandes refusées correspondantes n'encombrent plus le Journal.

9.2 Blocage des processus d'administration dangereux ICMP et IGMP

Si votre ordinateur fait partie d'un simple réseau local domestique, ou d'un réseau local plus important dont l'administrateur n'utilise pas les protocoles *ICMPv4, ICMPv6 et IGMP,* vous avez intérêt, pour des raisons de sécurité (cf. 1.4.5),

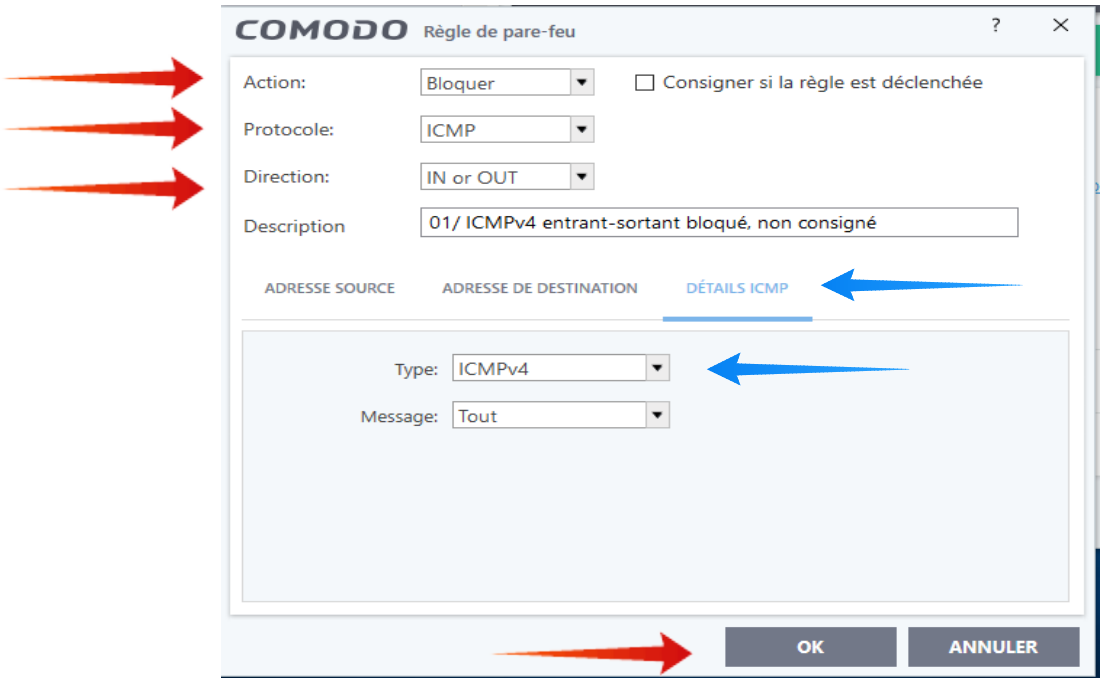
à bloquer les requêtes de connexions entrantes et sortantes pour ces protocoles ; dans le cas inverse vous conserverez la configuration de base décrite en 5.3.

Sous réserve de la condition ci-dessus, nous allons donc créer pour ces processus d'administration trois règles de blocage des connexions numérotées de 01/ à 03/ et que nous placerons **en tête de la fenêtre des règles globales** afin qu 'elles soient prioritaires : à titre conservatoire les 2 règles originelles *ICMPv4 entrant autorisé ne s*eront pas supprimées, mais elles deviendront inefficaces puisque situées en dessous de **la règle 01/ de blocage ICMPv4** que nous allons créer ci-dessous :



- dans la fenêtre des règles globales ci-dessus cliquez sur « + Ajouter », puis dans la fenêtre de la page suivante qui s'est ouverte, choisissez « Bloquer » en face d'Action, ICMP en face de Protocole, « IN or OUT » en face de Direction, renseignez la Description comme page suivante, sélectionnez « Détails ICMP », puis ICMPv4 pour

le type et validez en faisant « OK » en bas de cette fenêtre ;



- pour vérification vous pouvez consigner provisoirement cette règle jusqu'à ce que les connexions ICMPv4 bloquées apparaissent dans « Intrusions Réseau » ;

- **pour ICMPv6** : faites de même pour créer une règle de blocage spécifique en retenant ICMPv6 au lieu d'ICMPv4

- **pour IGMP** *:* dans la case « Protocole » choisissez, avec la flèche verticale, IP, puis, dans la rubrique « Détails IP », apparue à la place de la rubrique « Détails ICMP », sélectionnez IGMP dans la case « Type », enfin validez en faisant « OK ».

Ces trois règles n'étant pas consignées et étant placées au dessus de la règle globale « 22/ bloquant les demandes entrantes dont la source est dans Domicile #1 » que nous avons consignée permettent, en évitant l'encombrement du Journal par les demandes de connexions refusées pour ces services ICMP et IGMP, de surveiller les autres demandes de connexions refusées, c'est-à-dire de repérer :

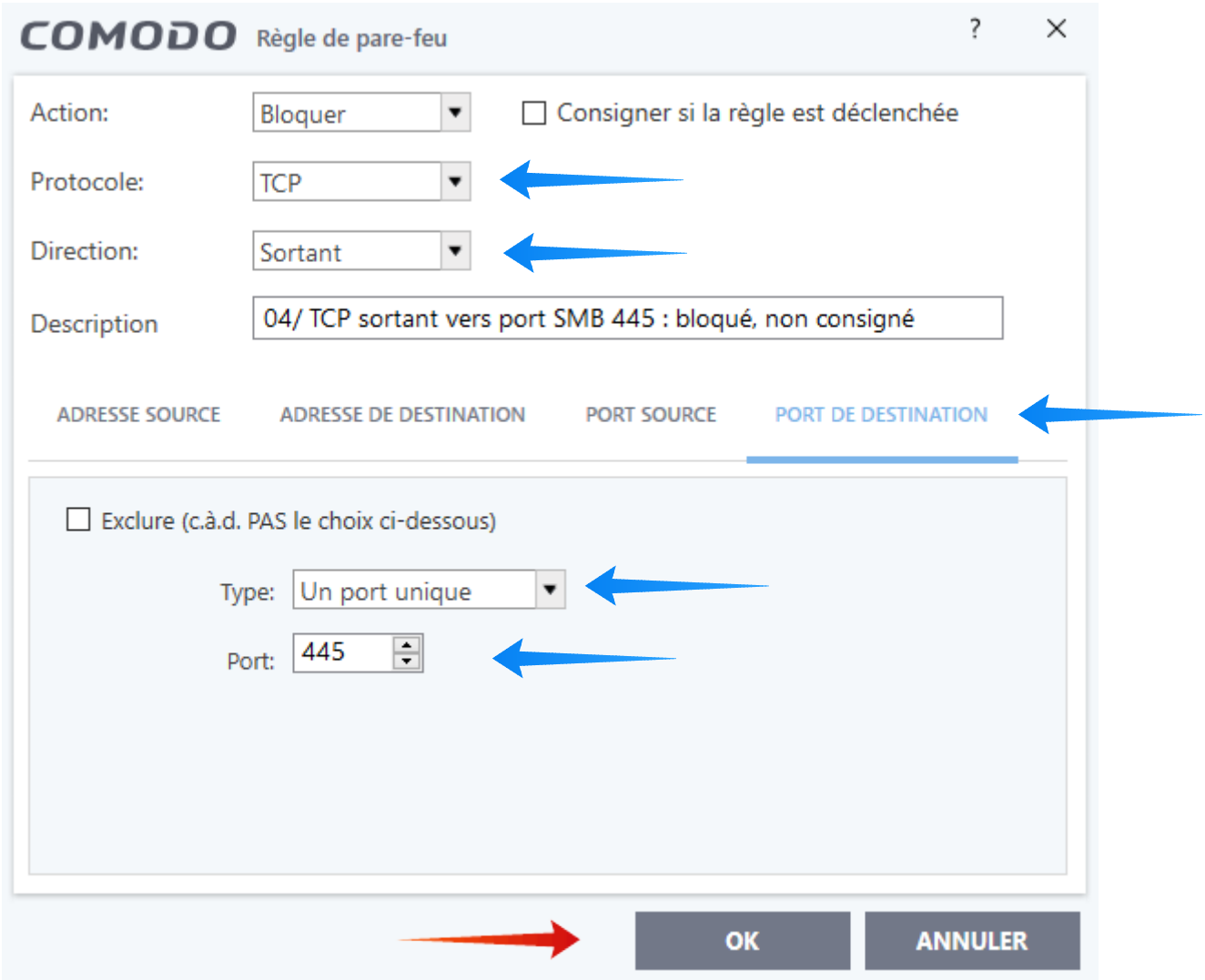
- les problèmes de connexions, par exemple lorsqu'une règle est mal configurée, ou n'est pas adaptée à l'utilisation ou l'installation d'un programme, d'une imprimante ;

- ou des connexions abusives et, moins souvent, d'éventuelles attaques de pirates ;

9.3 Blocage des services dangereux SMB, Netbios, SSDP et SNMP

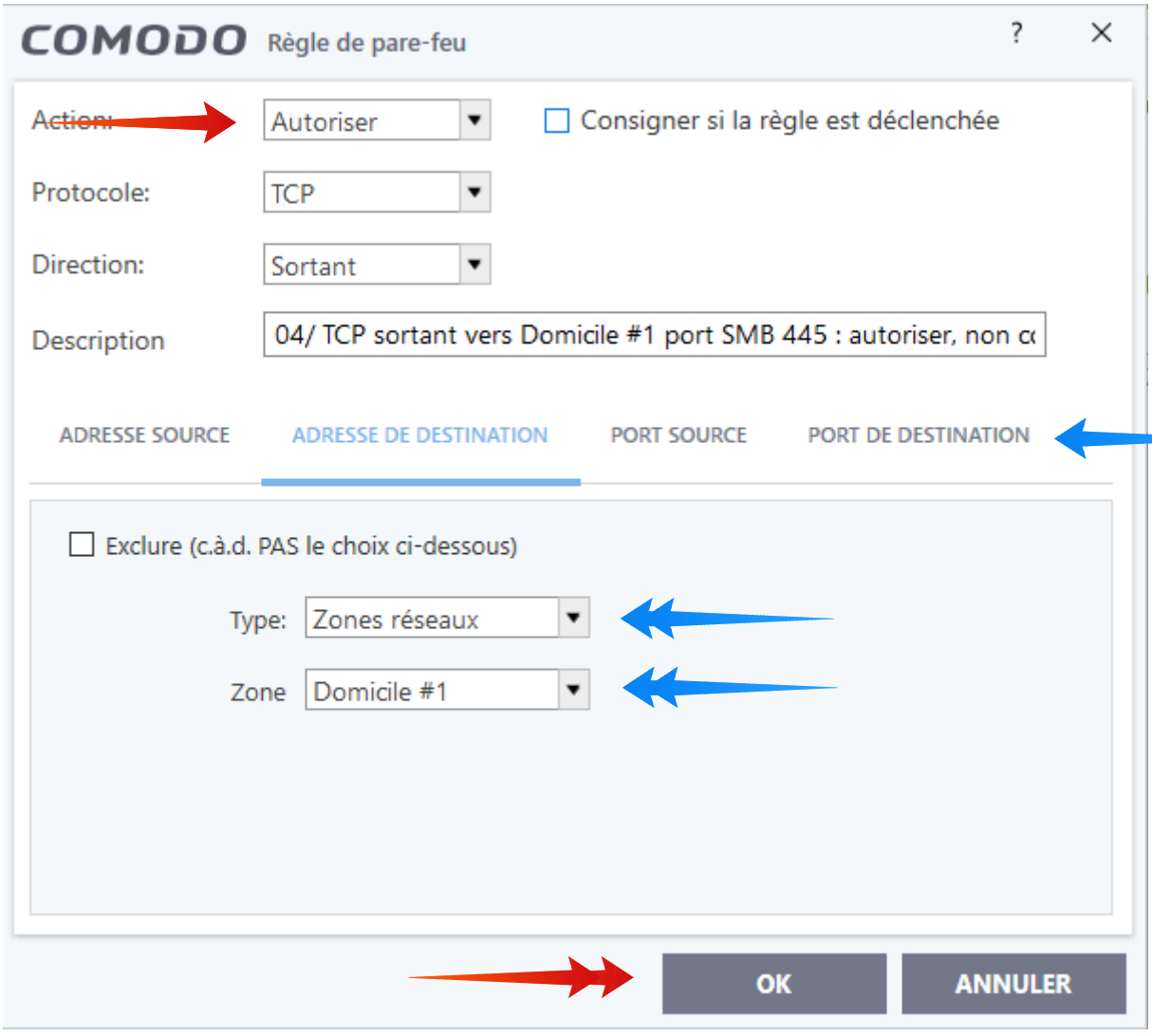
9.3.1 Le service SMB (cf. 1.4.7 f/) sera bloqué par la règle 04/ (tableau en 9.2)

- Action : Bloquer, non consigné ; - Protocole : TCP ; - Direction : Sortant ;
- Description : « 04/ TCP sortant vers port SMB 445 : bloqué, non consigné » ;
- Port de destination : 445 ; les adresses source, de destination et le port source seront laissés dans leur configuration par défaut.



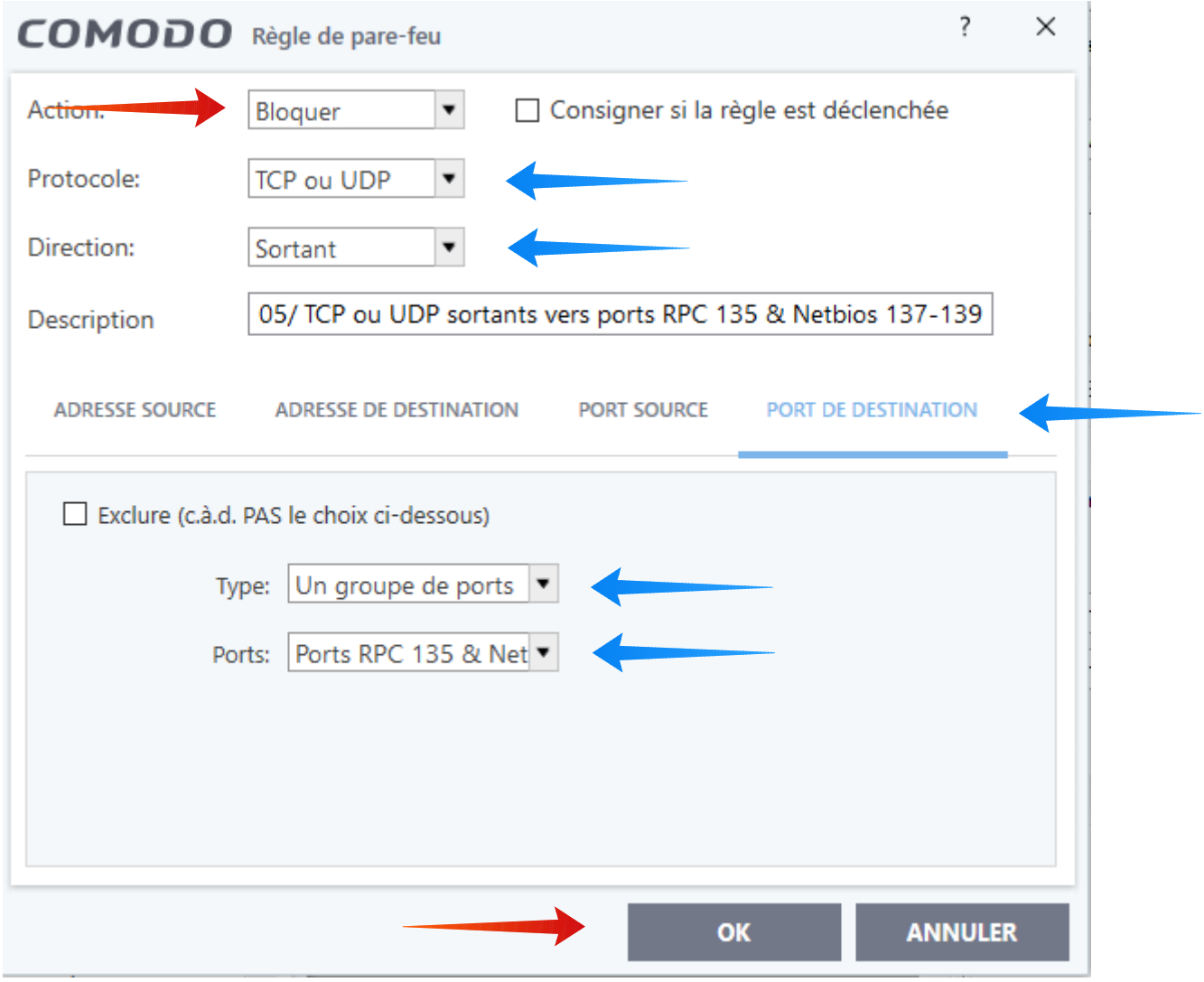
Si des partages de fichiers ou d'imprimantes sont indispensables (mais cela fragilise la sécurité de l'ordinateur), cette règle de blocage sera remplacée par une règle d'autorisation **vers la seule zone locale** :

- Action : Autoriser, non consigné ; - Protocole : TCP ; - Direction : Sortant ;
- Description : « 04/ TCP sortant vers Domicile #1, port SMB 445 : autorisé, non consigné » ;
- Adresse de destination, Type : Zone réseaux, Zone : Domicile #1
- Port de destination : 445 :



La **règle de blocage (ou celle d'autorisation) doit être placée au dessus de la règle 21/ régissant les demandes sortantes dont la cible est située au domicile.**

9.3.2 Le Système Netbios (cf. 1.4.7 g/) présente une très grave faille de sécurité, aussi faut-il interdire toute connexion utilisant les ports RPC 135, Netbios 137 à 139 et SMB 445 en élaborant la règle 05/ de blocage pour le trafic TCP ou UDP sortant sur ces ports, paramétrée selon la figure ci-dessous. Pour ce faire on utilisera le groupe de ports Netbios, créé précédemment en 8.5.



9.3.3 Le service SSDP (cf. 1.4.7 g/), qui utilise UDP sur le port 1900 en unicast ou en multicast, est potentiellement vulnérable, aussi, dans la fenêtre des règles globales, cliquons sur « Ajouter », pour créer la nouvelle règle 06/ qui suit :

- Action : **Bloquer, ~~consigné~~** ; Protocole : **UDP** ; Direction : **Sortant** ; Description : *« 06/ UDP sortant vers port 1900 (SSDP) : bloqué, non consigné » ;* **Port de**

destination : 1900 ; les adresses source, de destination et le port source peuvent être laissés dans leur configuration par défaut.

En complément seront désactivés SSDP, l'Hôte de périphérique UPnP et Service Partage réseau du Lecteur Windows Media (cf. Annexe B - Gestion des services Windows)

Il sera toujours possible d'autoriser temporairement ces demandes de connexions et de revenir sur ces réglages si cela s'avérait nécessaire pour l'installation d'un équipement particulier (imprimante ou routeur UPnP, par exemple).

9.3.4 Le service SNMP, particulièrement dangereux a enfin été retiré de Windows 10 depuis la version 1809. Il est indispensable de le désactiver sur les versions antérieures de Windows (cf. Annexe D : Désactivation du protocole SNMP) et de bloquer (règle 07/) les demandes de connexions sortantes en direction des ports UDP 161 et 162.

9.3.5 Les demandes de connexions entrantes pour les services dangereux de ce paragraphe 9.3 ne nécessitent pas de règles spécifiques car elles seront bloquées par la règle 22/ **que nous avons transformée** (en 9.1.2) **en règle** « Bloquer & consigner les demandes entrantes provenant de la zone locale (Domicile # 1) ».

9.3.6 A la fin de cette configuration, lancer une sauvegarde « Fw 12_cfg Niveau 1 du ... » qui pourra être utilisée en cas de problème.

10 Niveau 2 de sécurité – Gestion des règles de programmes

Ce niveau 2 permet à l'utilisateur expérimenté d'utiliser les alertes pour contrôler directement par lui-même la création des règles de programmes ce qui nécessite :

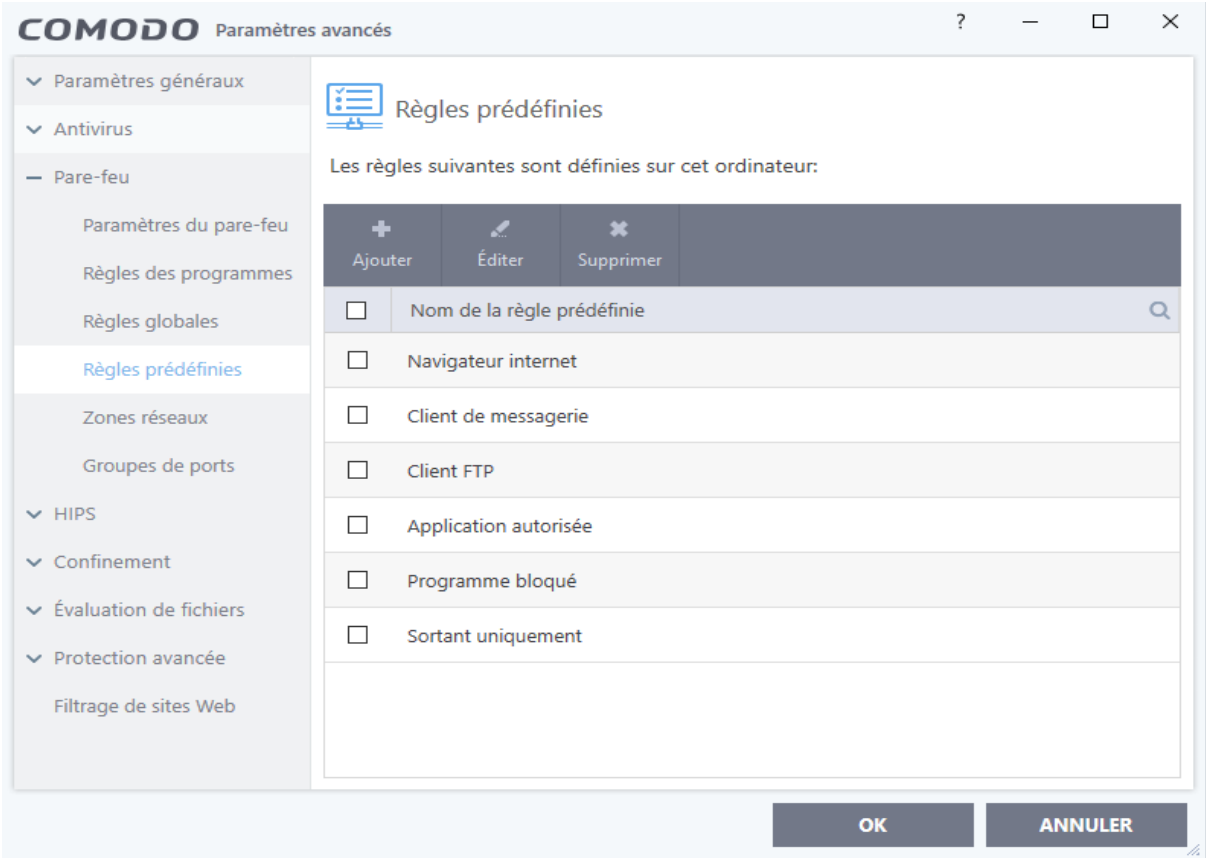
- de prendre connaissance du paragraphe précédent afin de savoir utiliser les outils que sont les alertes et la consultation des « Journaux » ;

- de sécuriser deux règles prédéfinies et d'en créer deux nouvelles afin de limiter le nombre des alertes et ainsi de faciliter l'utilisation du mode personnalisé ;

- de passer du mode dit sécurisé au mode personnalisé qui permet, grâce aux alertes, un meilleur contrôle de la gestion du pare-feu.

10.1 Les règles prédéfinies

L'emploi des règles prédéfinies facilite l'utilisation du mode personnalisé : en effet une règle prédéfinie regroupe en une seule règle l'ensemble des autorisations et des blocages de connexions que pourrait solliciter une application pour un, plusieurs ou l'ensemble des protocoles (TCP, UDP, IP , …) vers un, plusieurs ou l'ensemble des ports permettant ainsi qu'il n'y ait qu'une alerte par application, lors de leur première requête, et non une multitude d'alertes pour chacun des protocoles ou ports utilisés.



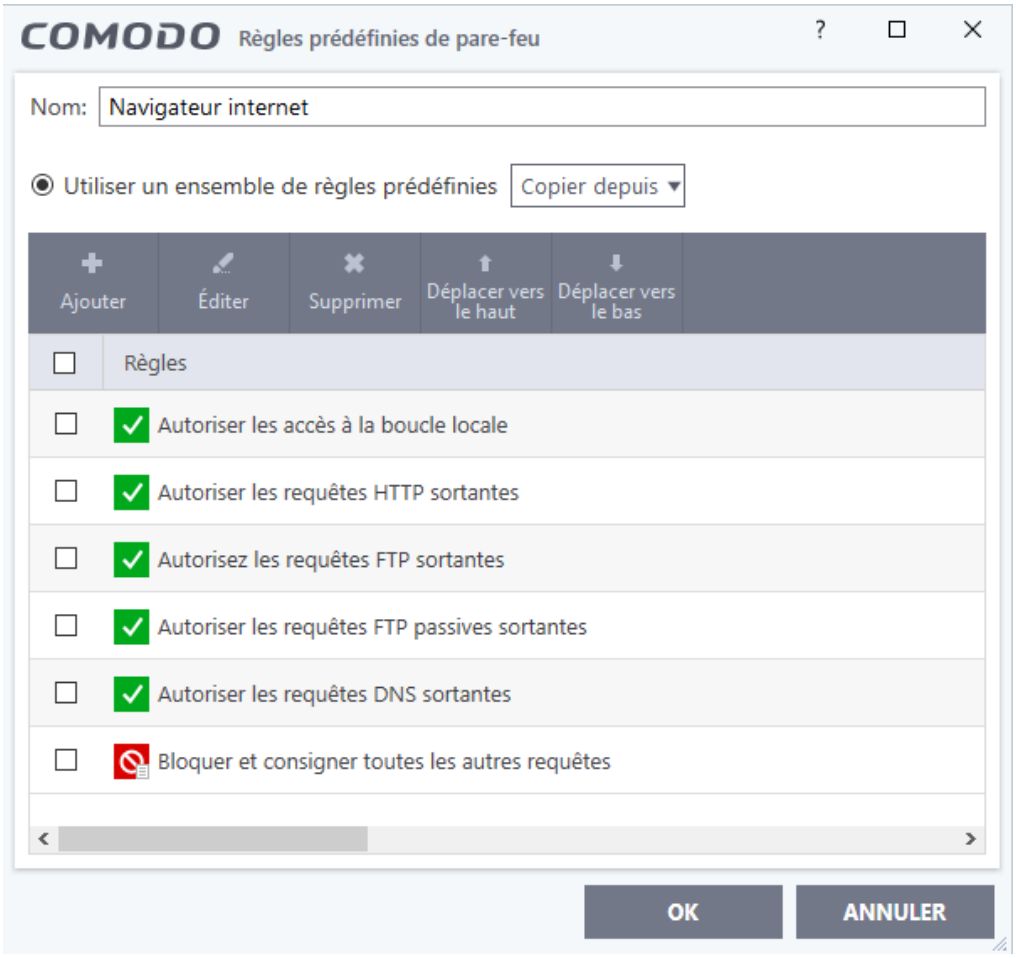
Avant d'employer les règles prédéfinies par défaut ci-dessus, il est préférable :

- **dans une première étape**, de sécuriser trois de ces règles prédéfinies préexistantes afin d'accroître la sécurité de l'ordinateur, et d'en créer deux nouvelles qui faciliteront la gestion des réponses aux alertes en les rendant moins fréquentes ;

- **puis, dans une seconde étape**, car cela est judicieux bien que non indispensable, de les classer dans un ordre qui facilitera leur utilisation en réponse à une alerte.

10.1.1 Première étape : sécurisation des règles prédéfinies

10.1.1 a/ Sécurisation de la règle « Navigateur internet »



La règle prédéfinie ci-dessus permet qu'il n'y ait pour l'emploi de chaque navigateur qu'une seule alerte, lors de la première requête de connexion de celui-ci.

- Afin de la sécuriser, si vous ne désirez pas utiliser le dangereux protocole de transfert de fichiers FTP, cliquez successivement sur chacune des deux sous-règles dédiées aux requêtes FTP et choisissez de les bloquer et de les consigner ;
- sinon, par souci de sécurité, spécifiez dans les deux sous-règles concernées les adresses sources et destinations que vous utiliserez (cf. 10,1,1 c/ ci-dessous).

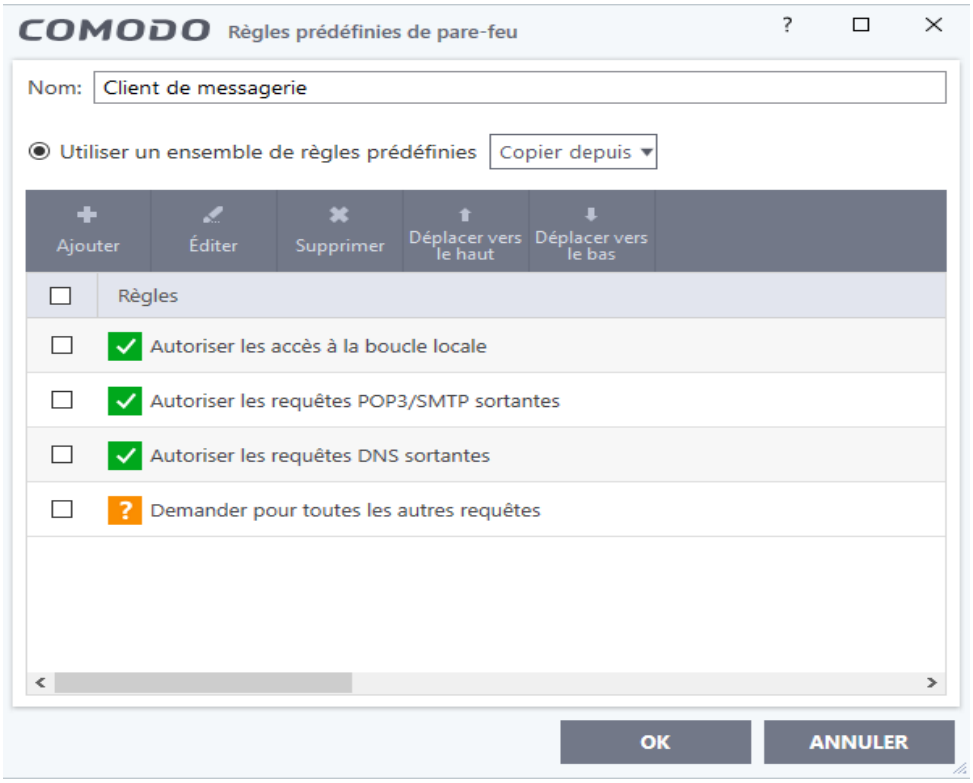
- De même *les utilisateurs expérimentés* n'utilisant pas un proxy fonctionnant avec *le port 8080, lequel peut être sujet à piratage (cf. 4.5), peuvent modifier la sous-règle HTTP en remplaçant le groupe de ports de destination 80 + 443 + 8080 par un*

groupe de ports 80 + 443 qu'ils auront créé ;

- Les utilisateurs de Chrome peuvent ajouter une règle autorisant UDP vers le port 443, mais cela ne semble pas indispensable.

- La règle « Navigateur internet », avec ses six sous-règles, est la plus complète des règles prédéfinies, elle peut être utilisée afin de modifier certaines règles prédéfinies ou d'en créer de nouvelles par copie (cf. 10.1.1 d/ et 10.1.1 g/).

10.1.1 b/ Maintien en l'état de la règle « Client de messagerie »

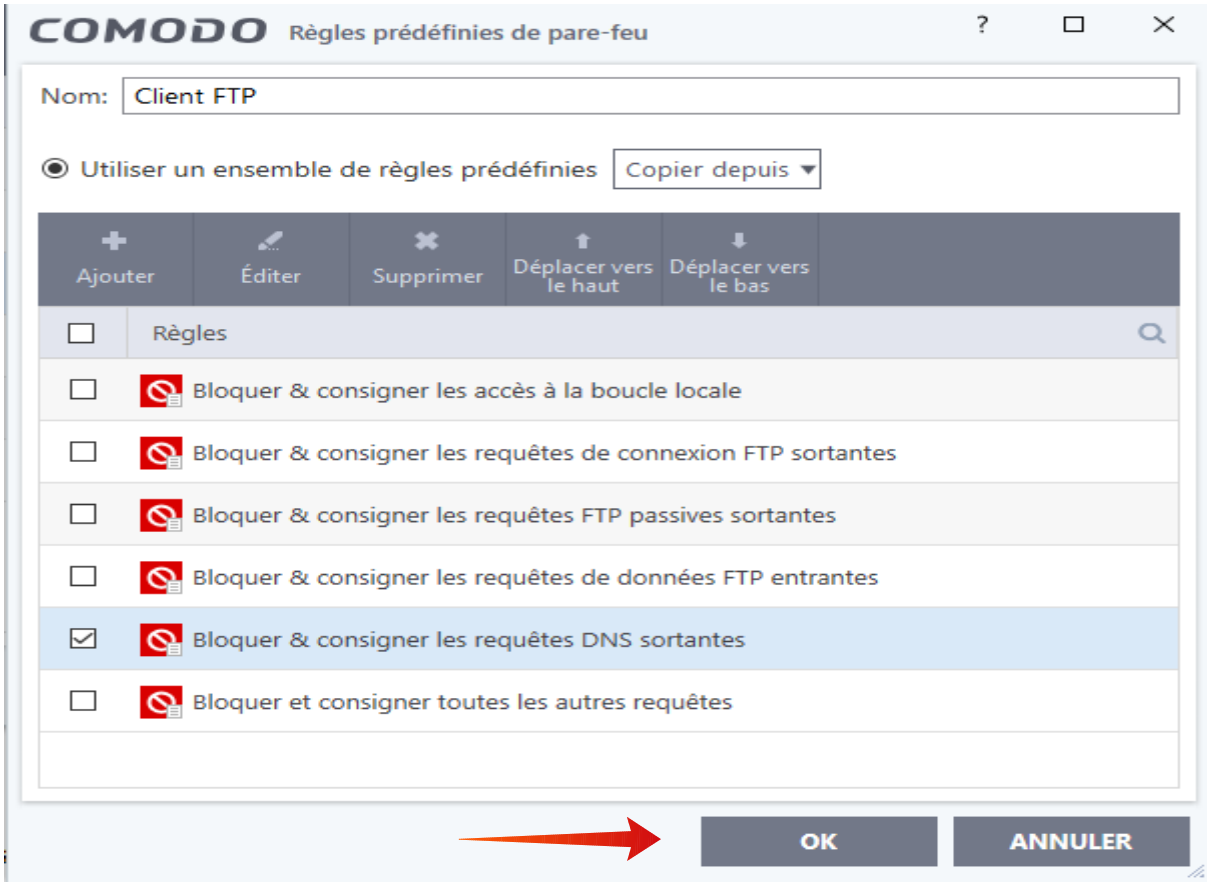


Il n'est pas nécessaire de modifier cette règle ; la dernière sous-règle permet l'ajout, si nécessaire, de toute sous-règle nécessaire, pourvu que vous l'autorisiez ; ainsi Thunderbird, utilisé avec les messageries Free et Gmx, nécessite également des connexions vers les ports 80 et 443 : la sous-règle « Demander pour toutes les autres requêtes » engendrera une demande d'autorisation pour les connexions vers ces ports et votre réponse « Autoriser » entraînera l'ajout par Comodo des sous-règles d'autorisations nécessaires pour les connexions en direction de ces ports ; dans le tableau des règles de programmes, l'intitulé en face de la règle Thunderbird se transformera alors automatiquement de « Client de messagerie » en **« Personnalisé ».**

10.1.1 c/ Sécurisation de la règle « Client FTP »

Employée telle quelle cette règle ouvrirait votre ordinateur à tous vents en autorisant notamment les connexions entrantes en provenance de toute adresse :

- si vous n'utilisez pas le protocole FTP : bloquez et consignez toutes les sous-règles de cette règle prédéfinie comme ci-dessous, puis cliquez sur OK *:*

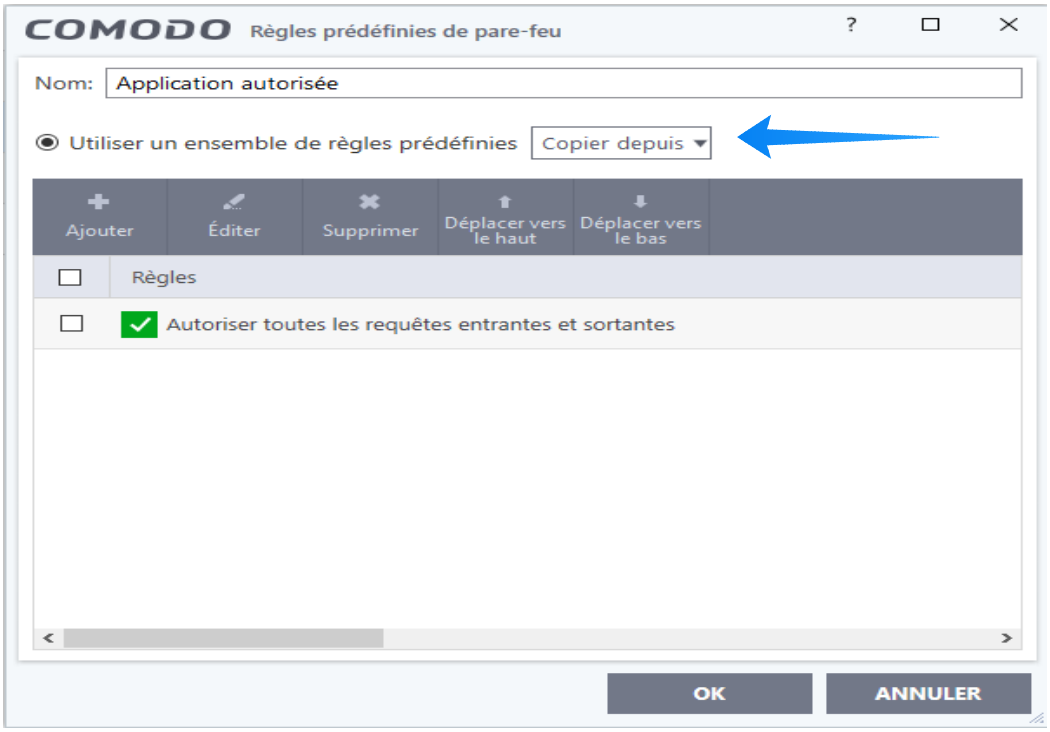


- si vous désirez utiliser le protocole de transfert de fichiers FTP, il est fondamental, pour des raisons de sécurité, de spécifier notamment dans les trois sous-règles dédiées à FTP, les adresses sources et destinations : les renvois aux ouvrages où vous trouverez les explications sur les dangers de FTP et les précautions à prendre, qui sortent du cadre de ce tutoriel de base, sont mentionnés en 1.4.7 h/ ;

10.1.1 d/ Sécurisation de la règle « Application autorisée » en « Application limitée autorisée »

La règle « Application autorisée » est trop dangereuse, car elle autorise toutes les requêtes entrantes et sortantes ; aussi doit-elle être modifiée comme il suit :

- cliquer sur la règle, puis sur « Editer », on obtient la fenêtre ci-dessous :

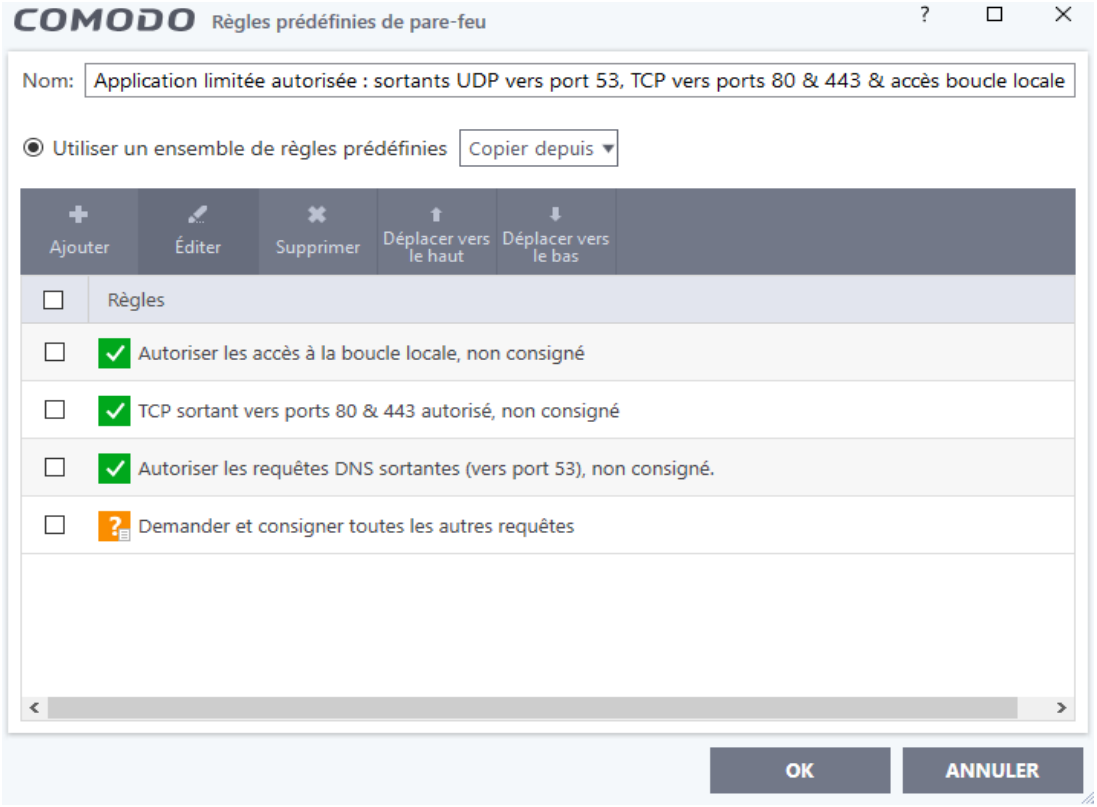


- puis, dans cette fenêtre ci-dessus, pointer dans la case **« Copier depuis »**, sur la petite flèche verticale orientée vers le bas ; cliquer ensuite sur « Règle prédéfinie », puis, dans le menu qui s'ouvre, retenez la règle prédéfinie « Navigateur internet » :

- les sous-règles de « Navigateur internet » sont instantanément retranscrites : parmi celles-ci supprimer les deux sous-règles FTP ;
- puis modifier la sous-règle de blocage en remplaçant dans le cadre Action «Bloquer » par « Demander » et intituler cette sous-règle « Demander et consigner pour toutes les autres requêtes » ; valider en faisant « OK »

- on obtient ainsi, comme sur la page suivante, une règle que l'on intitulera **« Application limitée autorisée »**, celle-ci autorisera toutes les connexions sortantes

TCP vers le groupe de ports HTTP 80, 443 (et éventuellement 8080) et UDP vers le port DNS 53, ainsi que toutes les requêtes d'accès IP sortant à la boucle locale (de 127.0.0.1 vers 127.0.0.1), les ports distants utilisés se situant dans la plage des ports dynamiques de 49152 à 65535 (cf. 1.3.8) :



- la sous-règle « Demander et consigner pour toutes les autres requêtes » engendrera une demande d'autorisation pour les connexions vers des ports autres que ceux précédemment spécifiés et votre réponse « Autoriser » engendrera l'ajout par Comodo des sous-règles d'autorisations nécessaires pour les connexions en direction des ports demandés ; dans le tableau des règles de programmes l'intitulé en face de la règle de l'application concernée se transforme alors automatiquement d'« Application autorisée » en « Personnalisé ».

Les connexions qu'autorise cette règle sont les plus utilisées par la majorité des applications et l'emploi de cette règle prédéfinie, lors de la première alerte déclenchée par la requête d'une application, évitera toutes les autres et parfois nombreuses alertes qui auraient autrement eu lieu lors de requêtes en direction de ces destinations.

10.1.1 e/ Maintien en l'état de la règle « Programme bloqué » (consigné)

10.1.1 f/ Maintien en l'état de la règle « Sortant uniquement »

Cette règle prédéfinie pré-existante est utilisée par défaut par « Comodo Internet Security » et par les « Applications Metro » :
- C:\Program Files\WindowsApps* et C:\Windows\system 32\WWAHost.exe.

A moins que vous ne sachiez parfaitement comment fonctionnent ces applications, **nous vous déconseillons fortement de modifier quoi que ce soit** à cette règle prédéfinie et à son utilisation.

Pour les autres applications que vous souhaitez autoriser il est préférable d'utiliser la règle « Application limitée autorisée » que nous avons obtenue en 10.1.1 d/.

Si vous envisagez de passer à la seconde étape, de déplacement des règles, ne créez pas les deux règles suivantes maintenant, mais seulement lors de cette seconde étape.

10.1.1 g/ Ajout de la règle « Programme bloqué non consigné » copiée à partir de « Programme bloqué (consigné) », puis modifiée

Afin de ne pas encombrer le Journal en utilisant la règle « Programme bloqué » (consigné), il est utile d'ajouter en bas du tableau des règles de programmes cette nouvelle règle qui sera obtenue à partir de la fenêtre des règles prédéfinies en cliquant sur « Ajouter » puis, dans la fenêtre qui s'ouvre, de pointer sur la petite flèche de **« Copier depuis »** et poursuivre, comme en 10.1.1 d/, en retenant la règle prédéfinie « Programme bloqué » (consigné), puis, dans cette copie, de décocher la case « Consigner si la règle est déclenchée » et de cliquer sur OK.

Cette nouvelle règle pourra souvent être utilisée pour les applications que vous n'utilisez pas et dont vous ne souhaitez pas qu'elles accèdent à Internet, par exemple pour des raisons de confidentialité, les applications Windows ComparTelRunner (télémétrie), Cortana et son acolyte SpeechRuntime, Zune Music, Your Phone, etc...

10.1.1 h/ Ajout de la règle « Programme bloqué, sauf accès autorisé à la boucle locale (loopback) : non consignés »

Cette nouvelle règle sera en général employée en réponse aux requêtes des applications non Windows que vous utilisez mais dont vous ne souhaitez pas qu'elles accèdent à internet, par exemple pour des raisons de confidentialité (logiciel de

photos, de généalogie, etc...) ou dans les cas où vous ne souhaitez pas la mise à jour de logiciels qui vous conviennent parfaitement dans la version que vous utilisez (logiciels C-Cleaner, Iobit Uninstaller, traitement de texte, etc...). **En effet cette règle autorise les demandes d'accès à la boucle locale, accès nécessaire au bon fonctionnement d'assez nombreuses applications (cf. 1.3.8).**

En dessous de la règle précédente, cette nouvelle règle sera copiée à partir de la règle prédéfinie « Navigateur internet » ; supprimez ensuite de la copie toutes les sous-règles qui ont été retranscrites sauf :
- « Autoriser les accès à la boucle locale » et
- « Bloquer et consigner toutes les autres requêtes » ;

puis intitulez la règle comme dans le titre et validez en faisant OK

10.1.2 Seconde étape (facultative) : déplacement des règles prédéfinies

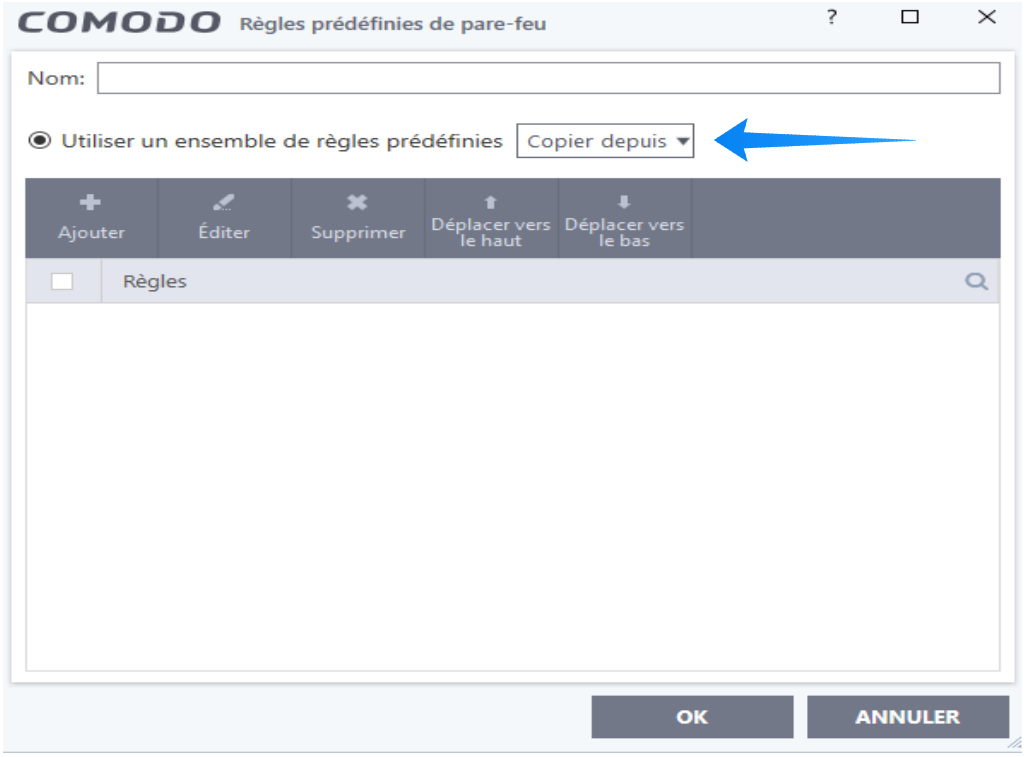
Cette seconde étape a pour objectif de classer les règles prédéfinies dans un ordre qui facilite l'accès aux plus utilisées lors des réponses aux alertes de pare-feu, ceci dans le seul but d'éviter de trop fréquents recours à l'ascenseur situé en bas de la fenêtre d'alerte ; étant sans incidence sur la sécurité, *vous pouvez renoncer à cette étape* si elle vous semble trop compliquée à mettre en œuvre, notamment lorsque de nombreuses règles de programmes ont déjà été associées à des règles prédéfinies, car il serait alors nécessaire de modifier en conséquence ces associations.

Avant de procéder à ce déplacement, nous allons au préalable numéroter les règles prédéfinies préexistantes de 1/ à 6/, en cliquant sur chacun de leurs intitulés et en validant à chaque fois par OK ; nous déplacerons ensuite les deux premières règles prédéfinies vers le bas de la fenêtre et nous utiliserons les emplacements libérés pour y placer les règles les plus utilisées qui seront ainsi plus aisément accessibles.

10.1.2 a/ Déplacement de la règle « 1/ Navigateur internet » en 7/

Cette règle, n'étant employée que lors de la première utilisation de chacun de vos navigateurs, peut sans inconvénient être déplacée en bas de la fenêtre des règles prédéfinies, en position 7/. Pour ce faire :
- dans la fenêtre des règles prédéfinies, cliquer sur « Ajouter » afin de créer cette nouvelle règle que nous intitulerons **« 7/ Navigateur internet »** ; dans la fenêtre qui s'ouvre pointez dans **« Copier depuis »** sur la petite flèche verticale orientée vers le bas ; cliquez sur « Règle prédéfinie », puis dans le nouveau menu qui s'ouvre, retenez « 1/ Navigateur internet » dont les sous-règles seront aussitôt automatiquement

retranscrites dans la nouvelle règle ; puis validez en cliquant sur OK **dans la fenêtre de cette nouvelle règle, ainsi que dans la fenêtre des règles prédéfinies** (ceci afin de conserver l'ordre des règles prédéfinies) ;
- ne supprimez pas la règle « 1/ Navigateur internet » à partir de l'emplacement de laquelle nous créerons une autre règle (cf. 10.1.2 c/) ;
- si vous avez déjà utilisé la règle prédéfinie 1/ lors de la création de règles de programmes, n'oubliez pas de modifier ces règles de programmes dans la fenêtre correspondante (cf. 10.4) en les associant à cette nouvelle règle prédéfinie 7/.



10.1.2 b/ Déplacement de la règle « 2/ Client de messagerie » en 8/

Au dessous de la règle précédente, créez une nouvelle règle intitulée « 8/ Client de messagerie » puis, par un processus identique au précédent, copiez la règle prédéfinie « 2/ Client de messagerie » ; faîtes « OK » deux fois comme en 10.1.2 a/ et ne supprimez pas la règle 2/ qui sera utilisée pour créer une autre règle (cf. 10.1.2 d/).

10.1.2 c/ Déplacement de la règle « Application limitée autorisée » en 1/

A partir de l'ancienne règle « 1/ Navigateur internet », précédemment copiée mais non supprimée, pointez dans **« Copier depuis »** sur la petite flèche verticale ; cliquez sur « Règle prédéfinie », puis dans le menu qui s'ouvre, retenez « 4/ Application

limitée autorisée » dont les sous-règles seront aussitôt retranscrites en 1/ que nous intitulerons **« 1/ Application limitée autorisée »** ; puis validez en cliquant sur OK .

10.1.2 d/ Création de la règle « 2/ Programme bloqué non consigné »

Créer cette nouvelle règle comme en 10.1.1 g/, mais à partir de l'emplacement de « 2/ Client de messagerie», en copiant **« Programme bloqué »,** puis en décochant « Consigner ... » dans cette copie et en cliquant deux fois sur OK comme en 10.1.2 a/

10.1.2 e/ Non déplacement des règles « 3/ Client FTP », « 5/ Programme bloqué » (consigné) et « 6/ IP sortant uniquement »

10.1.2 f/ Création de la règle « 4/ Programme bloqué, sauf accès autorisé à la boucle locale (loopback) : non consignés »

Créer cette nouvelle règle comme en 10.1.1 h/ mais à partir de l'emplacement de « 4/ Application autorisée » .

Au terme de ce périple, après vérification du fonctionnement de votre navigateur et de votre messagerie, nous disposerons des 8 règles prédéfinies ci-dessous, dont les règles 1/, 2/ et 4/, aisément accessibles, seront les plus utilisées :

10.2 Préliminaires au passage en mode personnalisé

Si vous envisagez les actions suivantes, il est préférable de le faire à ce stade :
- désinstaller les programmes inutilisés ;
- désactiver les services Windows dangereux ou inutiles (cf. Annexe B - Gestion des services Windows) ;
- désactiver les options de confidentialité qui ne sont pas nécessaires (cf. Annexe C - Gestion des options de confidentialité).

10.3 Passage du mode sécurisé au mode personnalisé et test de la configuration

Disposant désormais de règles prédéfinies adéquates nous pouvons passer du mode dit sécurisé de gestion du pare-feu qui accepte, pourvu qu'elles ne soient pas bloquées par une règle globale, toutes les demandes de connexions des milliers d'application jugées saines par Comodo, avec les risques que cela comporte si l'application autorisée est mal configurée ou si elle présente une faille de sécurité non corrigée lors d'une mise à jour, au mode personnalisé de gestion du pare-feu qui vous permet de n'autoriser que les connexions **des seules applications qui vous sont indispensables.**

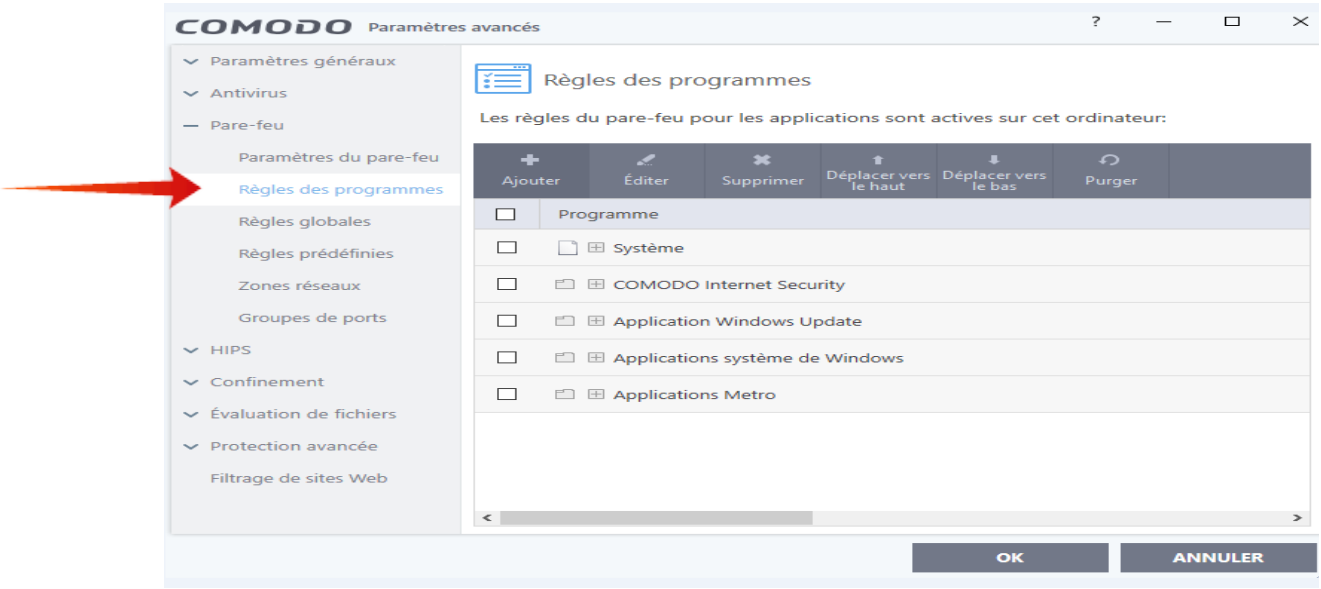
Après avoir retenu ce mode personnalisé dans la fenêtre d'accueil « Vue avancée » ou dans la fenêtre des paramètres du pare-feu, il est temps de tester cette configuration en lançant successivement vos applications les plus utilisées et en créant, par vos réponses aux alertes ainsi engendrées, les règles de programmes nécessaires associées aux règles prédéfinies adéquates suivantes :
- navigateurs : « Navigateur Internet » ;
- Thunderbird ou Outlook : « Client de messagerie » ;
- diverses fonctions de votre antivirus (mises à jours, analyses, recherche des vulnérabilités) : « Application limitée autorisée » ;
- logiciels de traitement de texte : « Application limitée autorisée » ou « Programme bloqué sauf accès à la boucle locale », selon que vous désirez que ces logiciels aient ou non accès à Internet.

Si un de ces programmes ne répond pas à la règle édictée, consultez le Journal et vérifiez la programmation de la règle prédéfinie correspondante, notamment qu'il n'y a pas erreur sur le protocole ou le n° du ou des ports distants autorisés.

Si tout se passe bien, lancez une nouvelle sauvegarde de la configuration que vous pourrez intituler « CIS_cfg Niveau 2 post règles prédéfinies, le ... ».

10.4 Les règles de programmes (cf. également [1] 12.2.2)

Rappelons que, en mode personnalisé, le pare-feu traite les demandes de connexions des applications *selon les règles déjà spécifiées par Comodo, pour les cinq règles pré-existantes ci-dessous* (qu'il est préférable de ne pas modifier), *ou par l'utilisateur* ; en l'absence de règle spécifiée, le pare-feu envoie systématiquement une alerte à l'utilisateur qui décidera si la demande doit être autorisée, bloquée ou traitée selon une règle prédéfinie, cette réponse engendrant la règle appropriée qui sera aussitôt placée au dessus des autres règles de programmes de la fenêtre ci-dessous.



A tout moment une règle, ou une sous-règle, peut être modifiée en cliquant dessus, en faisant « Editer », puis en modifiant les paramètres appropriés.

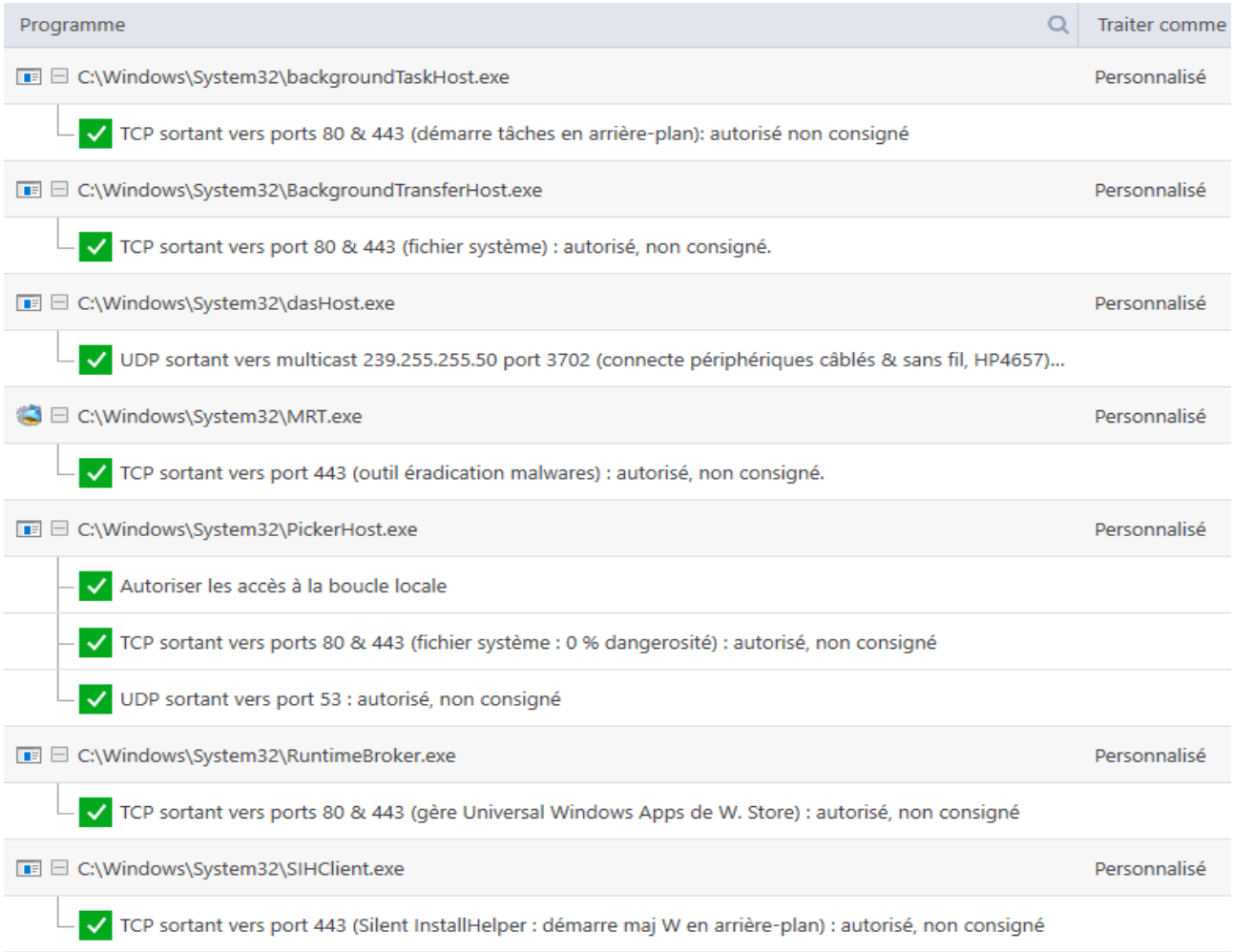
10.4.1 Règles de programmes pour les applications Windows

Le site de Malekal [14] conseille de bloquer les connexions pour les applications suivantes susceptibles d'être utilisées pour télécharger des logiciels malveillants : *powershell.exe ; wscript.exe ; mshta.exe ; rundll32.exe ; explorer.exe* (sauf vers le port 443), ainsi que les processus *Winword.exe* et *Excel.exe* afin de se protéger des macros malicieuses.

Selon vos besoins et désirs, vous pouvez aussi choisir **« Bloquer, non consigné »,** par exemple pour « ComparTelRunner.exe » (télémétrie), Cortana et ses applications associées « SpeechModelDownload.exe » et « SpeechRuntime.exe » si vous ne souhaitez pas utiliser Cortana, ainsi que pour les services de Microsoft Office si vous

utilisez un autre traitement de texte, etc...

Cependant si vous connaissez mal les diverses applications Windows et leurs fonctionnalités, **soyez prudent** et, afin d'éviter de bloquer une application qui pourrait être essentielle, cliquez sur « **Autoriser** » pour toute application Windows, signalée comme fiable par Comodo ; voici ci-dessous quelques règles d'autorisation pour des applications Windows (avec, dans le libellé, commentaire sur le rôle de l'application) :



10.4.2 Règles de programmes pour les applications non Windows

A la demande de connexion d'une application non Windows, on peut répondre :

a/ en bloquant l'application, en choisissant l'une des règles prédéfinies :

- *« 2/ Programme bloqué non consigné »* comme pour le logiciel de généalogie Myheritage que l'on ne veut plus utiliser, mais que l'on ne veut pas désinstaller ;

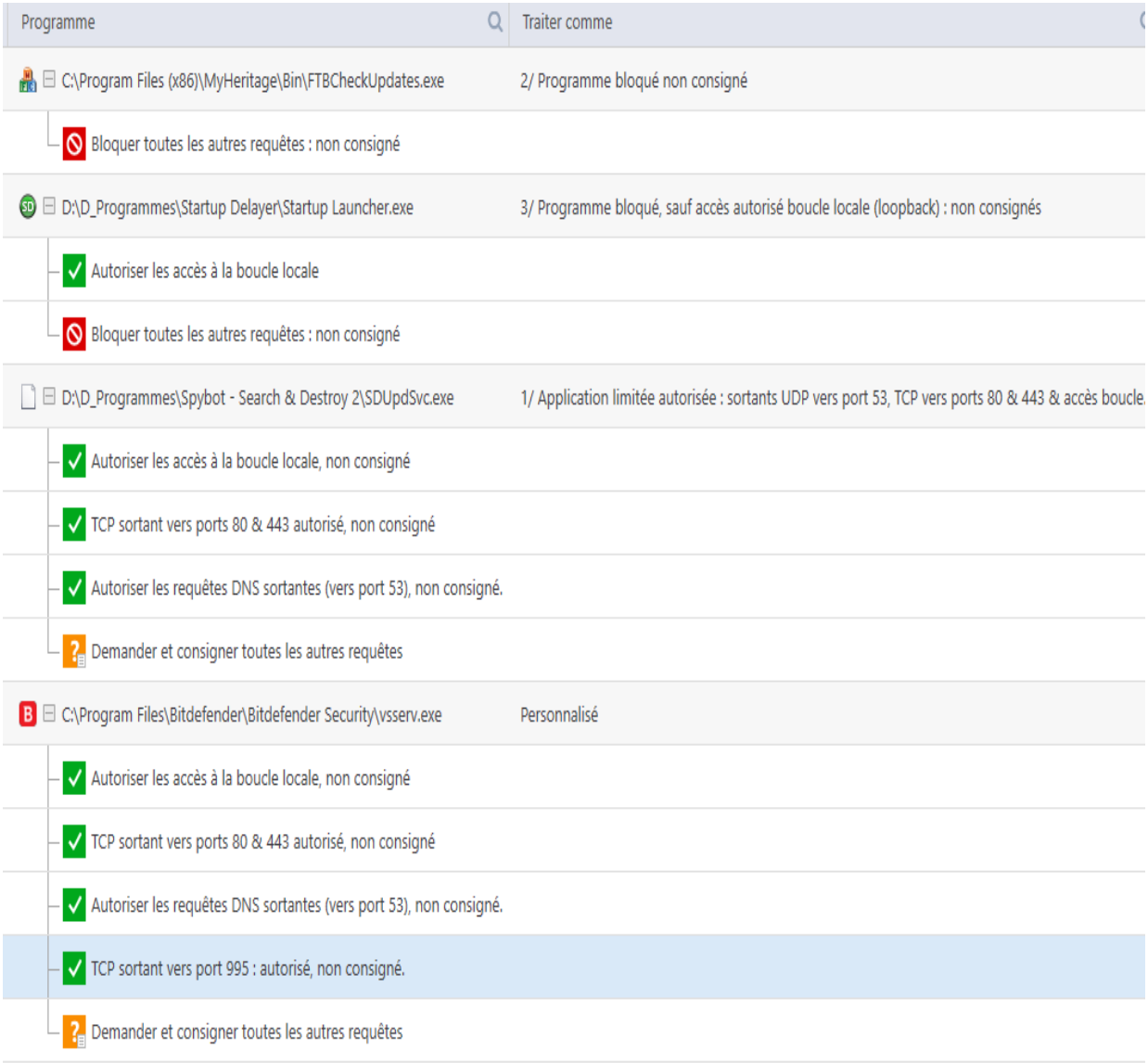
- *« 4/ Programme bloqué, sauf accès à la boucle locale »*, comme pour le logiciel StartUp Delayer, que l'on utilise, mais dont on souhaite interdire l'accès à Internet ;

b/ en autorisant l'application qui vous est indispensable et qui doit avoir accès à Internet (navigateur, messagerie, pare-feu, antivirus, etc.), avec la règle prédéfinie appropriée :

- *« 7/ Navigateur Internet », « 8/ Client de messagerie »* ou *« 3/ Client FTP »* ;

- *ou « 1/ Application limitée autorisée »* lorsqu'il s'agit d'une demande vers l'un des ports 80, 443, 53 ou pour l'accès à la boucle locale (de 127.0.0.1 vers 127.0.0.1) que l'on désire autoriser ;

- enfin simplement *« Autoriser »* lorsque l'on désire autoriser la connexion et que la demande pour celle-ci est en direction d'un autre port distant ou d'une autre destination que précédemment ; dans ce cas la règle est créée à destination de ce seul port, ou bien une sous-règle est ajoutée à la règle prédéfinie 1/ si celle-ci a déjà été utilisée pour cette application, comme en page suivante, l'autorisation « TCP sortant vers le port 995 » pour BitDefender.



10.4.3 Classement des règles de programmes

Les règles peuvent être déplacées en cliquant dessus puis en les faisant glisser jusqu'à l'endroit souhaité ou en utilisant les onglets « Déplacer vers le haut » ou « Déplacer vers le bas ».

Afin de retrouver facilement une règle il est préférable de les classer, dès que possible, avant qu'elles ne soient trop nombreuses. A titre indicatif, nous classons personnellement les règles de haut en bas de la façon suivante :

- règles récentes et en cours d'examen ;
- programmes non Windows autorisés ;

- programmes non Windows bloqués ;
- applications Windows autorisées ;
- applications Windows bloquées ;
- navigateurs Internet ;
- client de messagerie ;
- antivirus ;
- Comodo ;
- règles pré-existantes.

11 Niveau 3 de sécurité - Gestion générale des demandes de connexions sortantes et isolement de la zone locale

Avec le niveau 2 de sécurité l'utilisateur bénéficie déjà d'un bon niveau de sécurité. Les utilisateurs qui souhaitent exercer un contrôle étroit du trafic et qui sont suffisamment expérimentés pour maîtriser la connexion Internet (cf. Annexes A 1.2.1 et A 1.2.2) et l'éventuelle liaison Wi-Fi de leur imprimante pourront atteindre la sécurité optimale du niveau 3 en mettant en place des règles globales de gestion des connexions sortantes :

- vers Internet, afin de n'autoriser les connexions que vers les seuls ports distants indispensables aux applications que vous souhaitez réellement utiliser (navigateur, messagerie, imprimante, etc.) ;

- vers la zone locale, afin de mieux protéger l'ordinateur des *équipements connectés situés dans cette zone ;*

Le grand principe de la gestion des règles globales sortantes est le suivant :
- tout interdire en transformant les règles d'autorisations sortantes générale 61/ et vers le domicile 21/ en règles de blocages (cf. tableau des règles globales en 11.1 d/) ;
- et créer, *au dessus de celles-ci*, des règles d'autorisation des demandes sortantes vers les seuls ports distants ou destinations indispensables aux applications que vous souhaitez utiliser.

A titre préliminaire, et par précaution, on relèvera les « Détails » figurant en A 1.2.2 afin de pouvoir rétablir une connexion éventuellement désactivée.

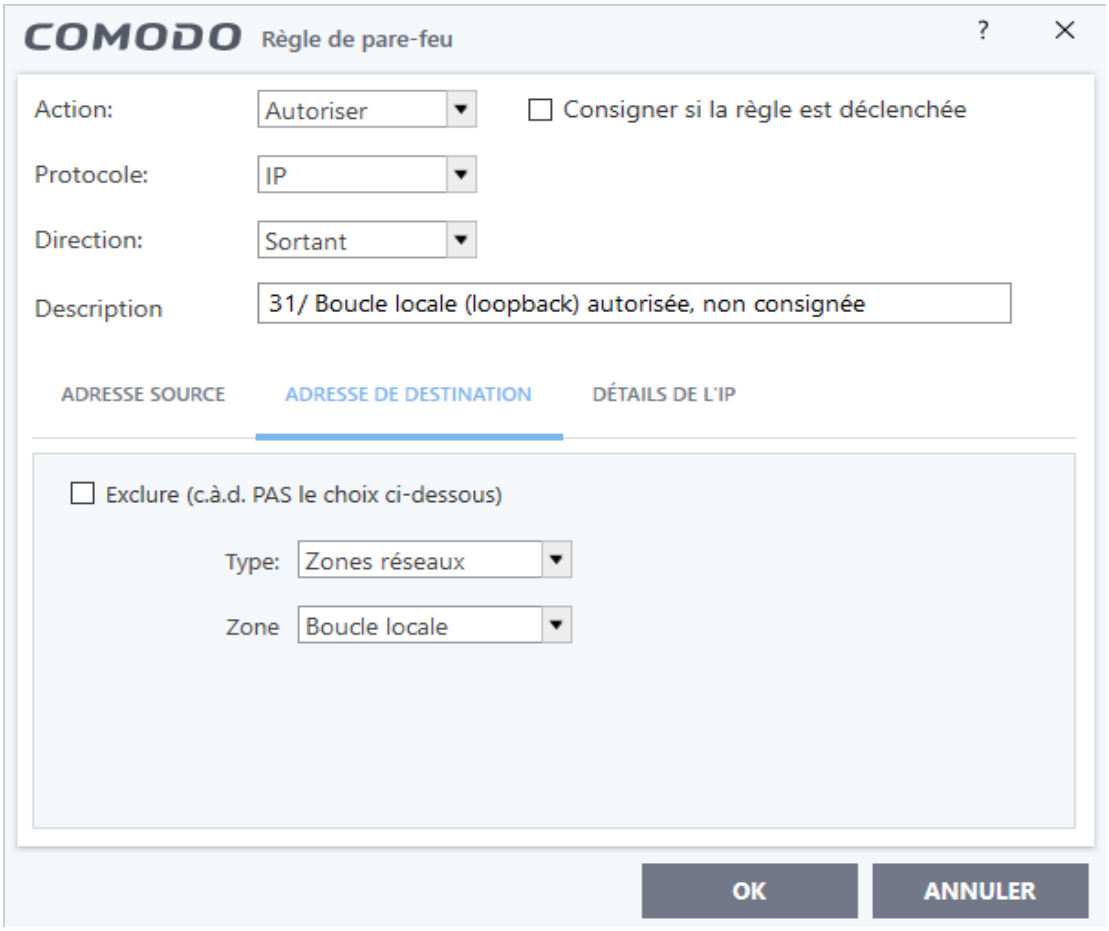
11.1 Règles globales de filtrage des connexions sortantes vers Internet

Après avoir transformé la règle d'autorisation sortante générale 61/ en règle de

blocage **consignée**, on créera au dessus d'elle les règles d'autorisations des demandes sortantes ci-dessous :

a/ pour l'accès à la boucle locale (loopback)

L'accès à la boucle locale étant nécessaire à de nombreuses applications afin que leur fonctionnement ne soit pas perturbé (cf. 1.3.8), on ajoutera à la fenêtre des règles globales (cf. en fin de 11.1 d/) la règle ***« 31 Boucle locale : autorisée, non consignée »***, comme ci-dessous :



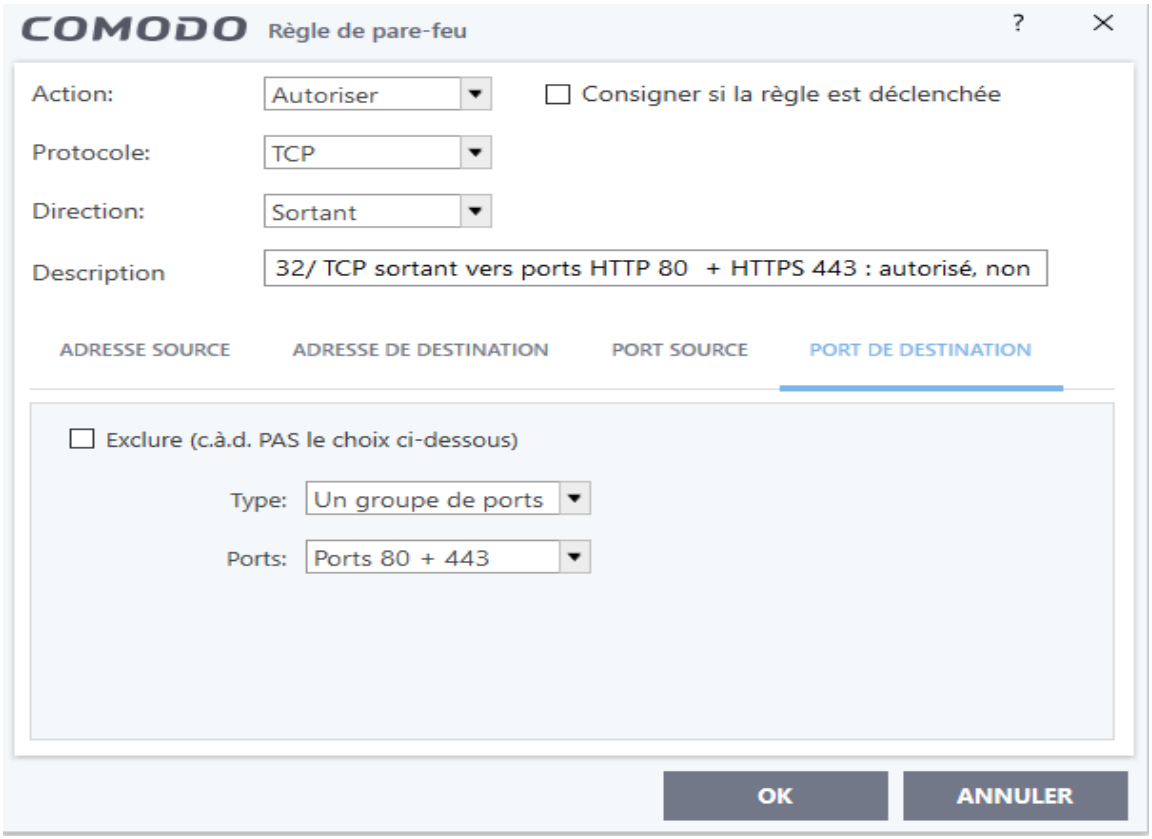
b/ pour l'accès au serveur DNS, indispensable pour accéder à Internet

Créer la règle *« UDP sortant vers port 53 : autorisé, non consigné. »*
ou bien, afin de limiter le détournement de DNS, ***créer deux règles globales 34a/ et 34b/ d'autorisation des connexions en direction du port 53 pour les seules***

destinations des deux serveurs mis à disposition par Comodo dont les adresses, en France métropolitaine, sont ***156.154.70.25 et 156.154.71.25*** (cf. 1.3.6).
note : en cas de modification intempestive de la connexion utilisée, la seconde solution peut entraîner la perte de l'accès à internet ; il suffit alors de revenir à la 1ère solution, ou, si vous êtes un tant soit peu expérimenté, de rétablir la connexion dans son état initial au niveau du « Centre Réseau et partage » (cf. Annexe A - Centre Réseau et partage A.2 Modifier les DNS).

c/ pour l'accès au Web : créer la règle ci-dessous

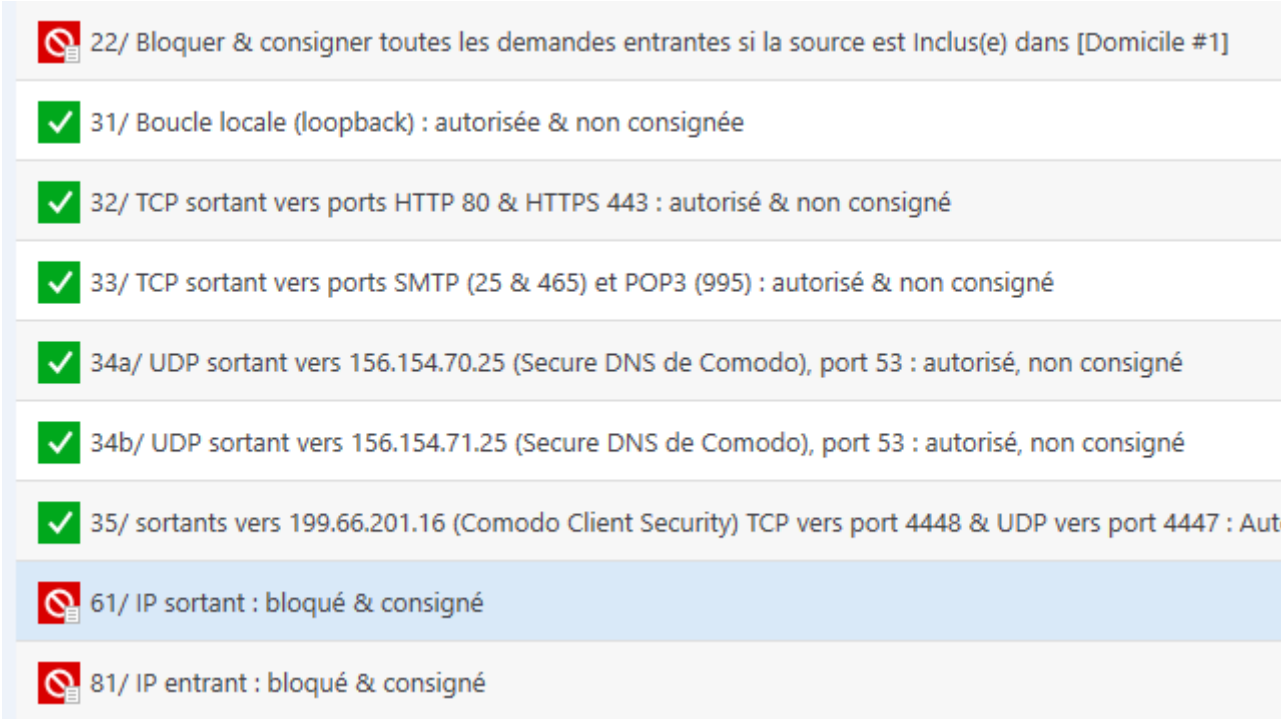
« 32/ TCP sortant vers ports HTTP 80 et HTTPS 443 : autorisé, non consigné », comme ci-dessous, le groupe de ports de destination retenu étant le groupe HTTP d'origine (80 + 443 + 8080), ou, si vous n'utilisez pas un proxy fonctionnant avec le port 8080, un groupe de ports (80 + 443), spécialement créé sans le port 8080, port sujet à piratage (cf. 8.5) ; *vérifier que le navigateur a bien accès à Internet.*



d/ pour l'accès au client de messagerie Si vous ne recueillez pas vos courriels directement sur la messagerie de votre fournisseur d'accès internet, mais par l'intermédiaire d'un client de messagerie tel Thunderbird ou Outlook, il est nécessaire

de créer la règle ***« 33/ TCP sortant vers ports POP3/SMTP : autorisé, non consigné »***, le groupe de ports de destination retenu étant le groupe de ports d'origine POP3/SMTP, ou, mieux, un groupe restreint que vous aurez créé et ne comprenant que les ports indispensables pour le client de messagerie que vous utilisez (cf. 1.4.7 c/ et d/) ; *vérifier que votre messagerie fonctionne.*

NOTE : par exemple, pour Thunderbird utilisé avec les messageries Free et Gmx, sont nécessaires les accès aux ports 995 (POP3), (25) et 465 (SMTP), 80 et 443 (HTTP et HTTPS) ; les ports non effectivement utilisés pourraient aussi être bloqués par des règles spécifiques ou une règle globale.



e/ pour le bon fonctionnement de Comodo

Créer la règle ***« 35/ TCP ou UDP sortant vers la destination 199.66.201.16, zone de ports 4447-4448 : autorisés, non consignés »*** (en fait TCP vers port 4448 et UDP vers port 4447).

11.2 Isolement des zones locales (Domicile #1 et éventuellement Domicile #2)

Autrefois les zones locales étaient considérées comme sûres, mais, suite à la multiplication des attaques à partir d'objets connectés au réseau local (objets divers tels que télévisions, smartphones et même imprimantes), il est désormais souhaitable de limiter au maximum, ou, mieux, de bloquer les liaisons de l'ordinateur aux objets connectés ; vous pouvez :

11.2.1 désactiver, s'ils ne vous sont pas indispensables, **ou sécuriser les partages de fichiers et d'imprimantes** (cf. Annexe A.4 Désactiver ou sécuriser les partages) ;

11.2.2 bloquer les demandes entrantes provenant d'une zone locale

En 9.1.2 nous avons déjà transformé *la règle d'autorisation des demandes entrantes provenant du domicile* en règle 22/ de blocage consigné de ces demandes entrantes ;

11.2.3 bloquer et consigner les demandes sortantes dont la cible est incluse dans la zone locale Domicile # 1, règle 21/ (et éventuellement Domicile #2, règle 21/bis)

Transformer *la règle d'autorisation des demandes sortantes dont la cible est incluse dans domicile #1 en règle « 21/ Bloquer et consigner les demandes sortantes dont la cible est incluse dans la zone locale »,* ce qui complète la règle 22/ de blocage des demandes de connexions entrantes originaires de la zone locale : **ainsi l'ordinateur sera-t-il isolé de tous les appareils connectés de la zone locale.**

L'examen d'« Intrusions réseau » (ou du journal du pare-feu) permettra de déterminer quelles règles d'autorisations il faut créer pour les seules applications concernant la zone locale que vous désirez utiliser ; *pour cela il est auparavant nécessaire* :

- que la case « Consigner si la règle est déclenchée » ait bien été cochée dans la règle 21/ ci-dessus ;

- que l'on décoche quelques temps « Consigner ... » dans la règle « 61/ IP sortant : autorisé, non consigné »), que l'on n'oubliera pas de cocher de nouveau ensuite.

Il ne reste plus, ensuite, qu'à créer, comme ci-dessous, les règles spécifiques d'autorisations nécessaires pour conserver l'accès à Internet, éventuellement aux partages auxquels vous souhaitez pouvoir accéder, et à l'imprimante.

Note 1 : rappelons que les imprimantes, **particulièrement lorsqu'elles sont connectées en Wi-fi** (par exemple pour l'approvisionnement en encre) peuvent être facilement piratées et contaminatrices des ordinateurs auxquels elle sont connectées ;

Note 2 : rappelons également que les objets connectés sont rarement sécurisés et qu'ils ne devraient pas être connectés directement à l'ordinateur (cf. 1.7).

11.2.3 A/ connexions à Internet :

- si vous n'avez pas désactivé le serveur DHCP de la box et attribué manuellement, dans la box, des adresses IP privées fixes à chaque appareil (cf. ci-dessous notes 2 et 3), le blocage des demandes sortantes vers la zone locale entraîne la perte de la connexion au serveur DHCP qui ne peut plus attribuer d'adresses IP privées aux appareils du réseau local : *l'accès à Internet est alors interrompu ;*

- la consultation d'« Intrusions réseau » (ou du journal du pare-feu) vous indique : *« Windows Operating System : Bloqué, Sortant, UDP, 0.0.0.0 port 68 vers 255.255.255.255 (adresse broadcast) port 67 » (DHCP Discovery) ;*

- pour rétablir la connexion à Internet il suffit, en général, d'ajouter la règle globale 16/ : *« Autoriser ; UDP ; Sortant ; de Toute adresse, port 68 ; vers 255.255.255.255 (broadcast) port 67 »*, placée comme indiqué dans la fenêtre située en fin de ce paragraphe 11.2.3 A/ ; *s'assurer que l'accès à Internet est bien rétabli.*

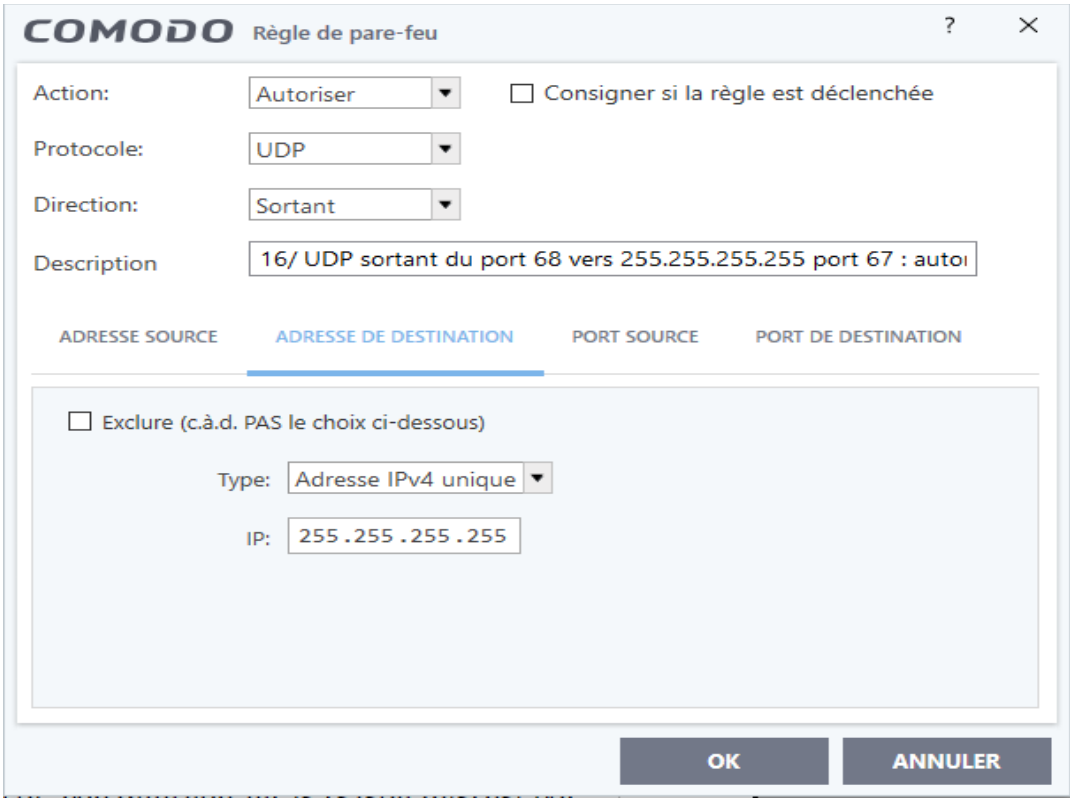
- note 1 : dans l 'Adresse source « de Toute adresse » s'il s'agit d'un ordinateur portable ; pour un ordinateur fixe on pourrait peut-être, être plus sélectif : « Zones Réseaux » puis « Domicile #1 » : à essayer éventuellement ;

- note 2 : 255.255.255.255 est l'adresse de broadcast (diffusion uniquement vers l'ensemble des machines d'un réseau local, non diffusion sur le réseau Internet par les box et routeurs) ;

- note 3 : les adresses IP privées attribuées se situent dans la plage 192.168.0.0 à 192.168.255.255 ;

- note 4 : si la connexion n'était pas rétablie il faudrait renseigner manuellement les adresses de la connexion précédemment relevées (cf. A 1.2.2 a et c) ou, plus aisément, les rétablir ainsi : activer le pare-feu Windows, désactiver un moment le pare-feu Comodo, se connecter à Internet ce qui rétablira la connexion, réactiver le

pare-feu Comodo et enfin désactiver le pare-feu Windows ;



- note 5 : si votre ordinateur demeure toujours dans le même lieu (avec la même box) et que vous êtes tant soit peu expérimenté vous avez intérêt à désactiver DHCP (cf. 1.4.7 e/ et « Annexe A - Centre Réseau et partage A.1 Désactiver DHCP ») : les adresses IP de vos équipements n'étant plus allouées par DHCP, mais étant fixes, vous bénéficiez alors des avantages suivants :

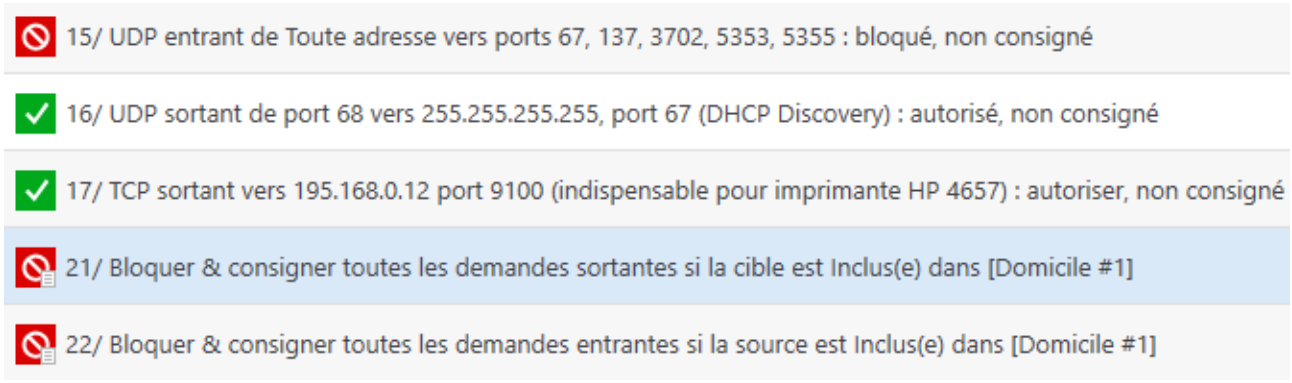
= la connexion au service DHCP n'étant plus nécessaire, ***la connexion Internet n'est pas interrompue ;***

= vous pourrez créer certaines règles de façon plus sélective car vous pourrez mentionner de façon précise les adresses des objets connectés qui ne varient plus à l'expiration d'un bail alloué par le système DHCP ;

= enfin votre ordinateur ne pourra plus être la cible d'attaques de type « DHCP Starvation » ou « DHCP Rogue ».

- la consultation d' « Intrusions réseau » signale ici le blocage « d'UDP **entrant** de 0.0.0.0, port 68 vers 255.255.255.255, port 67 » : s'agissant d'une connexion entrante cette

connexion sera bloquée (règle 15/ : cf. 12), ce qui n'aura d'ailleurs pas d'incidence négative sur l'accès à Internet (cf. également 12/).



11.2.3 B/ liaison à l'imprimante

a/ la liaison filaire (à privilégier) **à l'imprimante n'est pas interrompue** par la règle de blocage des connexions sortantes vers la zone locale ;

b/ la liaison Wi-Fi (dangereuse, plutôt à éviter) **à l'imprimante est interrompue**

- par exemple, pour une imprimante HP 4650, reliée en Wi-Fi, la consultation d'« Intrusions réseau » (ou du journal du pare-feu) vous indique :

Windows Operating System : Bloqué, Sortant, TCP, 192.168.0.10 port 51825 vers 192.168.0.12 port 9100 ; l'ordinateur ayant dans ce cas l'adresse IP 192.168.0.10, l'imprimante, l'adresse IP 192.168.0.12, et le port source étant un port dynamique compris entre 49152 et 65535 (ici 51825) ;

Windows Operating System : Bloqué, Sortant, UDP, 192.168.0.10 port 59197 vers 192.168.0.12 port 161 ;

Windows Operating System : Bloqué, Sortant, UDP, 192.168.0.10 port 57979 vers 239.255.255.250 port 3702 ;

Windows Operating System : Bloqué, Sortant, UDP, 192.168.0.10 port 5353 vers 224.0.0.251 port 5353 ;

et *Windows Operating System : Bloqué, Sortant, UDP, 192,168,0,10 port 60385 vers 224.0.0.252 port 5355*

- dans la configuration de notre ordinateur, pour rétablir la liaison à cette imprimante HP, on constate qu'autoriser la première de ces demandes de connexion et la placer au dessus de la règle 21/ de blocage des connexions sortantes dont la cible est incluse dans le domicile suffit à rétablir la liaison :

aussi est-il souhaitable de n'ajouter que la règle globale « 07/ *Autoriser ; Sortant ; TCP ; de Zone locale vers port 9100 »,* et de la placer au dessus de la règle 21/**;**

- Note : des règles de blocage non consignées pour les quatre autres demandes de connexions, et également placées au dessus de la règle 21/, pourraient être créées afin d'éviter d'encombrer inutilement le journal du pare-feu (cf. 12)

- pour une autre configuration ou une autre imprimante, le processus utilisé pour la liaison Wi-Fi pourrait être différent : la règle ajoutée doit alors autoriser le processus bloqué tel que relevé dans « Intrusions réseau » ; par exemple « *Autoriser ; Sortant UDP ; de Zone locale vers 224.0.0.251, port 5353 » (cf. 1.3.7).*

11.2.3 C/ Liaisons aux autres objets connectés :

- la perte de connexion de votre ordinateur avec les autres équipements connectés est l'objectif recherché, puisque la sécurité de la plupart des objets connectés n'est actuellement que très rarement assurée, ce qui devrait inciter à les connecter séparément à l'aide d'un routeur ou d'un routeur VPN (cf. 1.7) ;

- à défaut, et à la rigueur, il ne faut donc créer de règle, *selon le même processus que précédemment,* que dans des cas où cela est indispensable, pour des ordinateurs, smartphones ou tablettes et même téléviseurs suffisamment sécurisés (codes PIN modifiés, écrans verrouillés, mises à jour régulières et antivirus spécifiques). Cette règle doit être la plus restrictive possible, et pour cela il est préférable d'attribuer à chaque objet connecté une adresse IP fixe et donc de désactiver DHCP si votre ordinateur est fixe (cf. 11.2.3 A/ : note 4).

Pour conclure n'oubliez pas :

- de vérifier que les règles 21/ et 61/ pour les connexions sortantes sont bien consignées ;

- que toutes les demandes pour des connexions entrantes pour DHCP, pour toute imprimante ou tout autre objet connecté doivent être bloquées ;

- de faire une sauvegarde de cette configuration que vous pouvez intituler par exemple « CIS_cfg Niveau 3, datée du ... »

12 Enregistrement dans le Journal des demandes entrantes (non indispensable)

Après la mise en place de la gestion des règles de programmes (10.4) et des règles globales pour les connexions sortantes (cf. 11.1), les plus expérimentés pourront désirer surveiller les nouvelles requêtes de connexions entrantes et les éventuelles attaques :

- pour cela, dans les fenêtres des règles de blocage pour les demandes entrantes, générale 62/, et pour le domicile 22/, nous allons cocher la case située devant « Consigner si la règle est déclenchée » ; nous observons alors dans le Journal du pare-feu les demandes **entrantes** suivantes de Windows Operating System, **protocole UDP** qui ont été bloquées :
= de 0.0.0.0 port 68 vers 255.255.255.255 port 67 (pour DHCP) ;
= de 192.168.0.12 (imprimante) port 137 vers 192.168.0.255 port 137 ;
= de 192.168.0.12 (imprimante) port 49186 vers 239.255.255.250 port 3702 ;
= de 192.168.0.12 (imprimante) port 5353 vers 224.0.0.251 port 5353 ;
= de 192.168.0.12 (imprimante) port 50560 vers 224.0.252 port 5355 ;

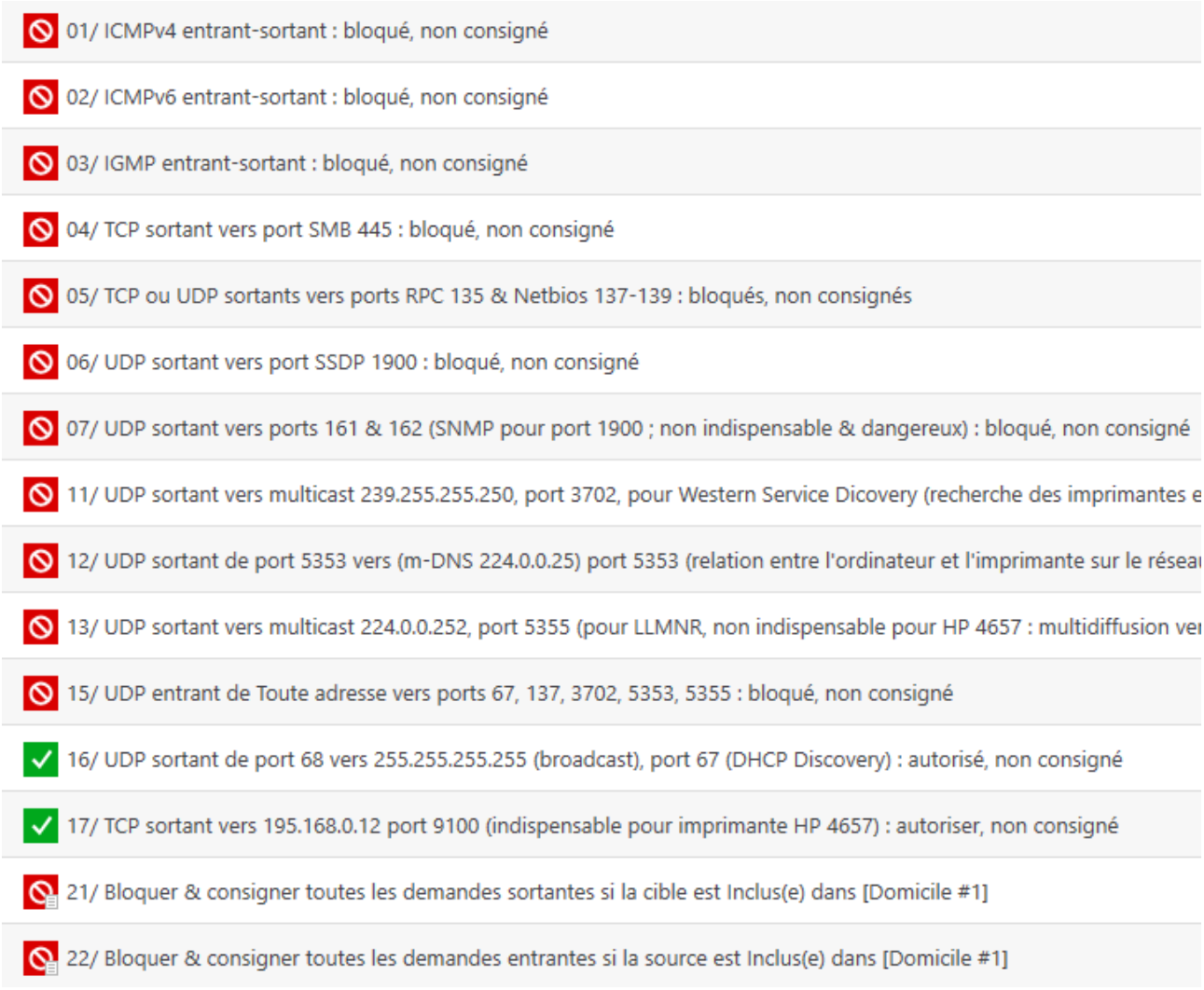
ces blocages n'empêchent pas DHCP et l'imprimante de fonctionner ; aussi, afin que le journal ne soit pas encombré par ces très nombreuses requêtes et reste aisément consultable pour surveiller d'éventuelles attaques ou d'éventuelles anomalies de configuration des règles, on peut créer un groupe des ports 67, 137, 3702, 5353 & 5355 , puis la règle « 15/ UDP entrant vers ports 67, 137, 3702, 5353, 5355 : bloqué non consigné » que nous placerons au dessus de la règle 22/ (cf. règle 15/ du tableau en fin de 11.2.3 A).

13 Récapitulation concernant le tableau des Règles globales

La partie inférieure du tableau des Règles globales figure à la fin de 11.1 d/ en page 66.

La partie supérieure du tableau des règles globales figure sur la page suivante ;
parmi ces règles peuvent être variables :
- la règle 04/ de blocage pour SMB 445 qui doit être transformée en règle d'autorisation vers la zone locale en cas de partages de fichiers ou d'imprimante ;
- la règle 16/ d'autorisation du port 68 vers le port 67 qui peut être transformée en

règle de blocage lorsque DHCP est désactivé ;
- les règles 11 à 13 et 17 qui dépendent de l'imprimante utilisée.



14 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 configurer rigoureusement et méthodiquement le pare-feu afin :
- de ne pas encombrer les Journaux d'événements car ceux-ci doivent demeurer facilement consultables et exploitables ;
- de privilégier le travail **en mode personnalisé** (niveaux 2 et 3 de sécurité) afin de n'autoriser que les services qui vous sont nécessaires ;

4/ de veiller à ce que tous les ports qui correspondent uniquement à des services qui ne vous sont pas nécessaires soient fermés grâce à une utilisation judicieuse des Règles globales ;

5/ de passer régulièrement en revue la configuration du pare-feu, particulièrement au niveau du tableau des Règles globales ;

6/ 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 ;
- 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;
- de mots de passe insuffisamment robustes ;
- des clefs USB et CD : analysez-les avec votre antivirus avant de les employer ;

Idéalement, si vous avez plusieurs ordinateurs il serait judicieux d'en réserver un, qui vous soit personnel, à vos opérations bancaires, achats et déclaration d'impôts en ligne et messageries : cet ordinateur serait relié en filaire à l'imprimante et ne serait

pas relié aux objets connectés ; il serait exclu des partages, ne serait pas utilisé pour les jeux en ligne et ne serait pas mis à disposition des enfants et adolescents.

N'oubliez pas l'importance de :

- la désinstallation des programmes inutilisés et la mise à jour sans délais de ceux amenés à se connecter à Internet (Windows, navigateurs, antivirus, …) ;
- la désactivation ou la sécurisation des partages de fichiers et d'imprimantes ;
- la désactivation de certains services de Windows dangereux ou inutiles, ainsi que de certaines fonctionnalités peu respectueuses de la confidentialité ;

Bonne route à vous sur les chemins du Web

Annexe A - Centre réseau et partage

Dans le module « Centre Réseau et partage » du « Panneau de configuration » de Windows on peut :

A.1 Désactiver DHCP

Si votre ordinateur est fixe et si vous êtes tant soit peu expérimenté, vous pouvez avoir intérêt à désactiver DHCP et à passer en baux DHCP permanents, pour cela :

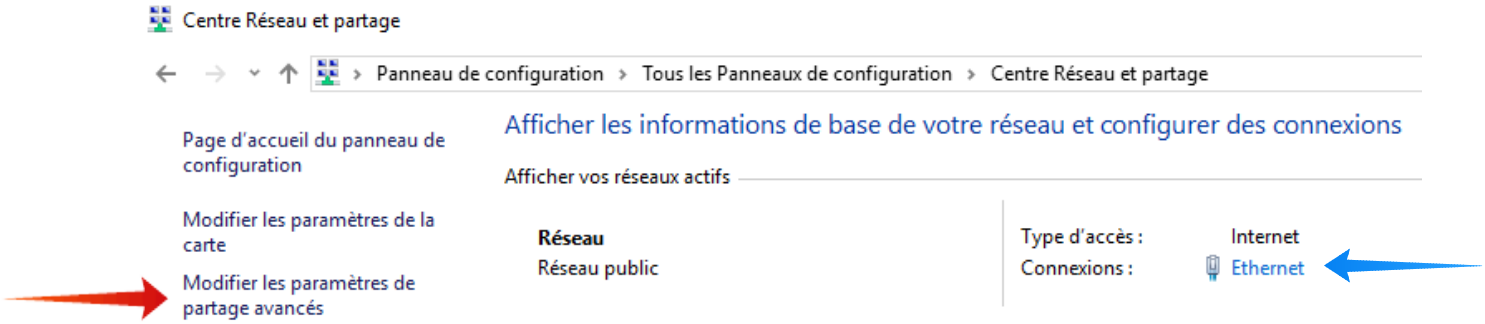
A.1.1 Etablir dans votre box la table de correspondances adresses IP/adresses MAC de vos équipements :

Par exemple pour la Freebox, entrez votre identifiant dans la barre de recherche de votre navigateur ; dans la fenêtre qui s'ouvre, entrez votre mot de passe :
- allez sur Gestion Freebox/Paramétrer mon routeur Freebox :
= Configuration du routeur : Etat : OUI ;
= Configuration du DHCP : OUI ;
= Redirection/baux DHCP/Baux DHCP permanents : établir la table de correspondance, en faisant correspondre par exemple chacune des adresses IP 192.168.0.11 à 192.168.0.xx à chacune des adresses MAC des équipements à connecter (les adresses MAC des ordinateurs se trouvent dans la fenêtre « Etat de (la connexion) » : cf A 1.2.2 a/ des deux pages suivantes ; l'adresse MAC d'une imprimante se trouve souvent dans la fenêtre de visualisation de cette imprimante ;

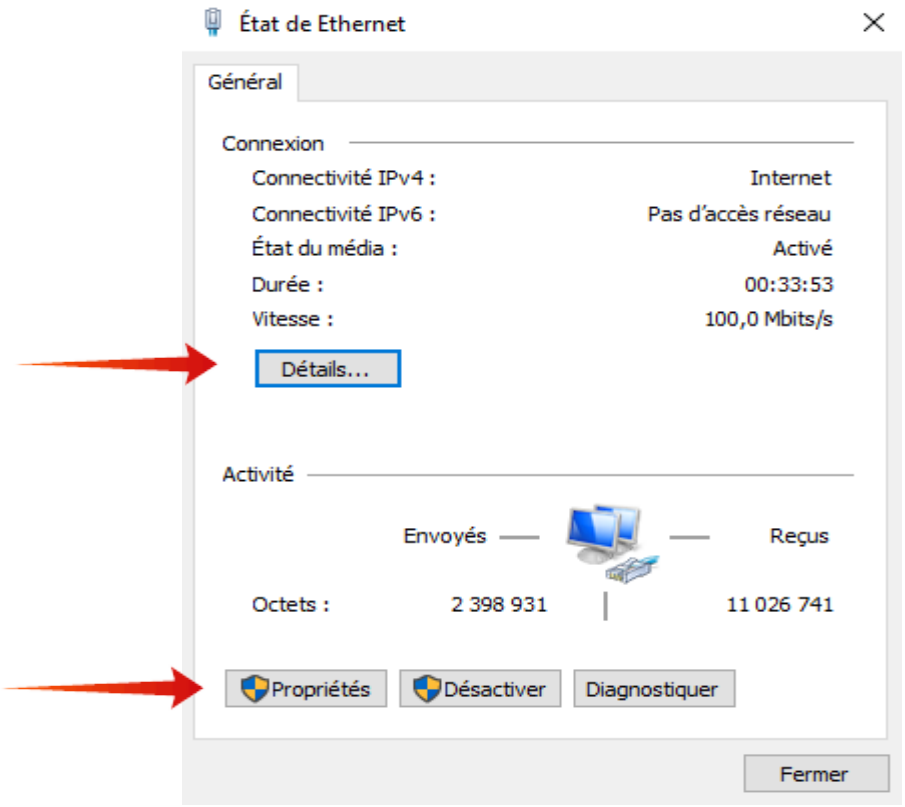
- sauvegardez la configuration en redémarrant la Freebox (l'éteindre puis la rallumer).

A.1.2 Désactiver (ou activer) DHCP sur l'ordinateur

A.1.2.1 Aller dans Centre de configuration\Centre Réseau et partage et cliquer sur votre connexion (ici, dans le tableau de la page suivante Ethernet : flêche bleue) :



A.1.2.2 dans la fenêtre qui s'ouvre

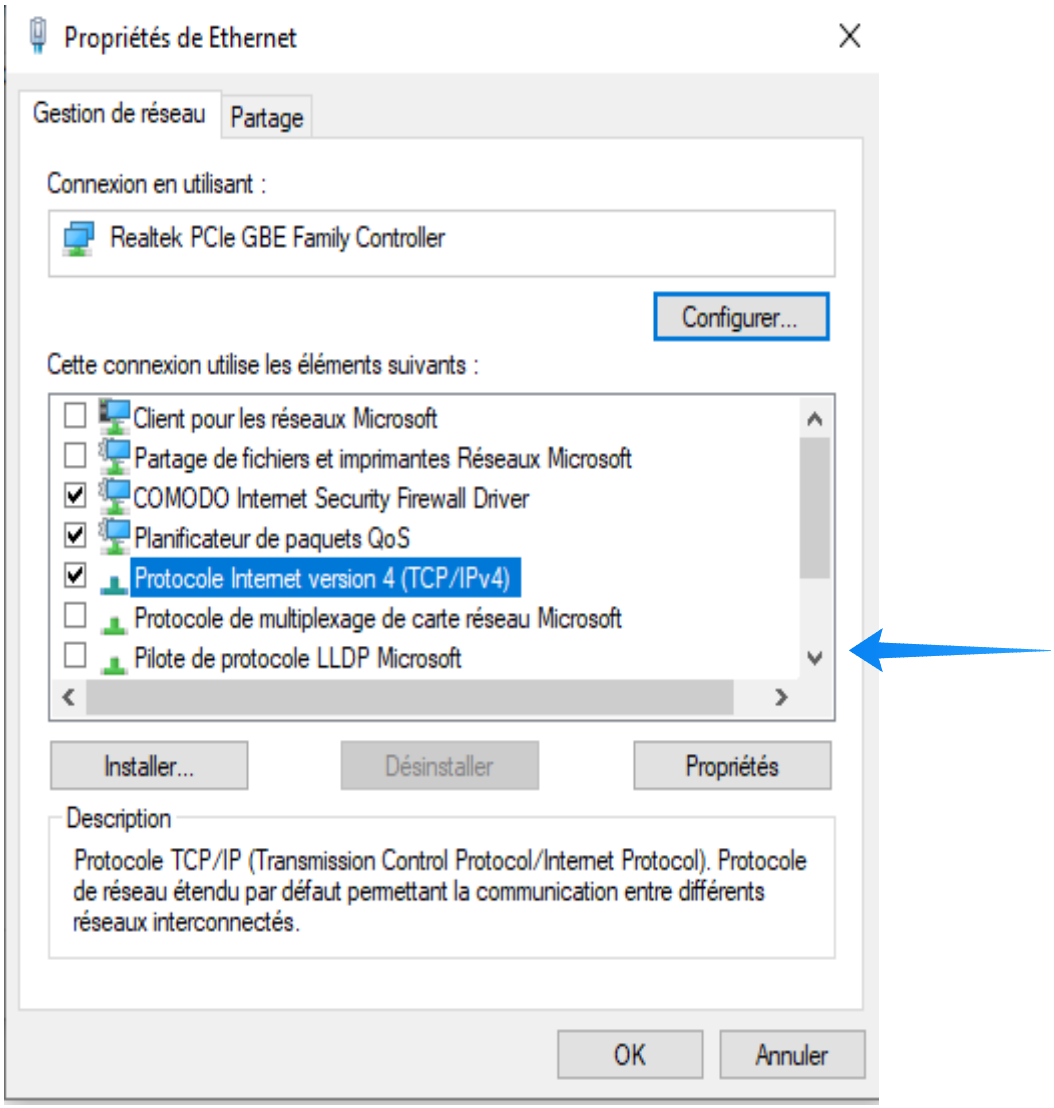


a/ en cliquant sur l'onglet « Détails » vous obtenez mentions :

- de l'adresse physique (adresse MAC) de l'ordinateur ;

- de l'état activé ou non de DHCP ;
- de l'adresse Ipv4 actuelle de l'ordinateur ;
- de l'adresse du masque de sous-réseau ;
- de l'adresse de la passerelle ;
- des deux adresses DNS en cours d'utilisation ;
- de l'état activé ou non de Netbios.

b/ en cliquant sur l'onglet « Propriétés » vous obtenez la fenêtre ci-dessous



c/ en surlignant « Protocole Internet version 4 » et en cliquant sur « Propriétés » vous obtenez une nouvelle fenêtre ou vous avez le choix entre :

- obtenir une adresse IP automatiquement (DHCP activé) ;

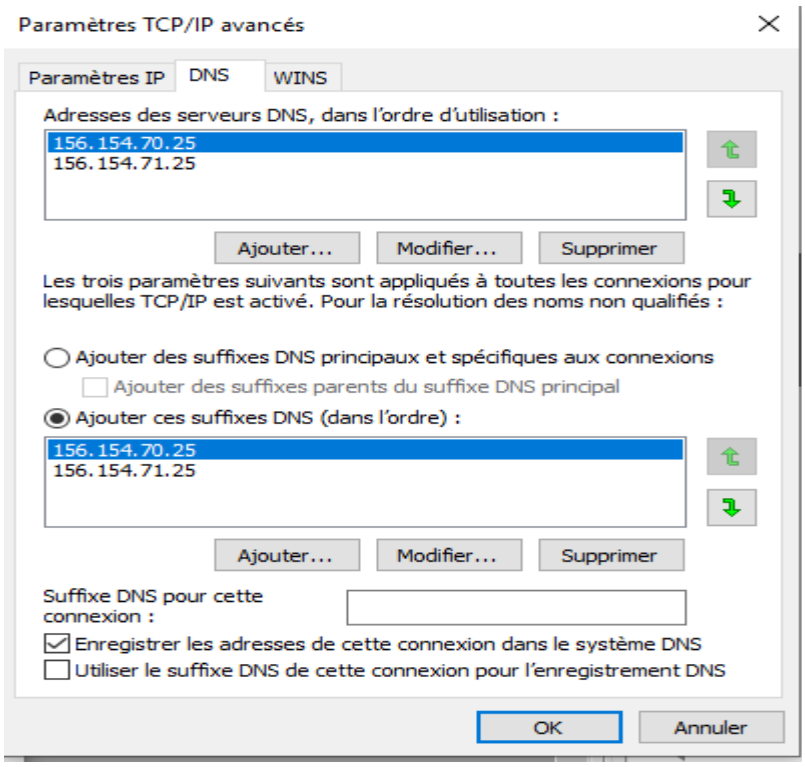
- ou utiliser l'adresse IP suivante (DHCP désactivé) : vous renseignerez l'adresse IP que vous avez choisie dans votre box ; et reprendrez le masque de sous-réseau et la passerelle par défaut mentionnés dans la fenêtre Détails de A 1.2.2 a/ ci-dessus ; faîtes alors OK pour valider ;

d/ l'onglet « Avancé » de la même fenêtre « Propriétés » vous conduit à une nouvelle fenêtre avec les trois onglets :

- « Paramètres IP » ;
- « DNS » conduisant à la fenêtre ci-dessous où l'on peut modifier les DNS ;
- « WINS » conduisant à une fenêtre en bas de laquelle on peut désactiver Netbios.

A.2 Modifier les DNS

- Dans la fenêtre « DNS » ci-dessous (obtenue en A 1.2.2 d/ ci-dessus), vous pouvez remplacer les adresses DNS attribuées par votre fournisseur d'accès Internet, par celles d'autres serveurs DNS, par exemple celles des serveurs COMODO sécurisés, ci-dessous celles de COMODO pour la France métropolitaine :



A.3 Désactiver Netbios

En bas de la fenêtre obtenue en cliquant sur l'onglet « WINS » ci-dessus, vous pouvez désactiver Netbios, mais, attention Netbios peut être réactivé par une mise à jour Windows, d'où l'intérêt de bloquer les connexions Netbios avec le pare-feu.

A.4 Désactiver ou sécuriser les partages [15]

Dans le module « Centre Réseau et partage », se rendre dans la colonne de gauche, sur « Modifier les paramètres de partage avancé » (cf. Annexe A 1.2.1 : flèche rouge) et désactiver, s'ils ne vous sont pas indispensables :
- les découvertes de réseau ;
- les partages de fichiers et d'imprimantes ;
- la multidiffusion en continu ;
- si le partage de fichiers vous est indispensable, utilisez le chiffrement 128 bits et activez le partage par mot de passe.
- dans tous les cas de désactiver SMB 1.0/CIFS dans « Programmes et fonctionnalités » / « Activer ou désactiver des fonctionnalités Windows » ;

Annexe B - Gestion des services Windows

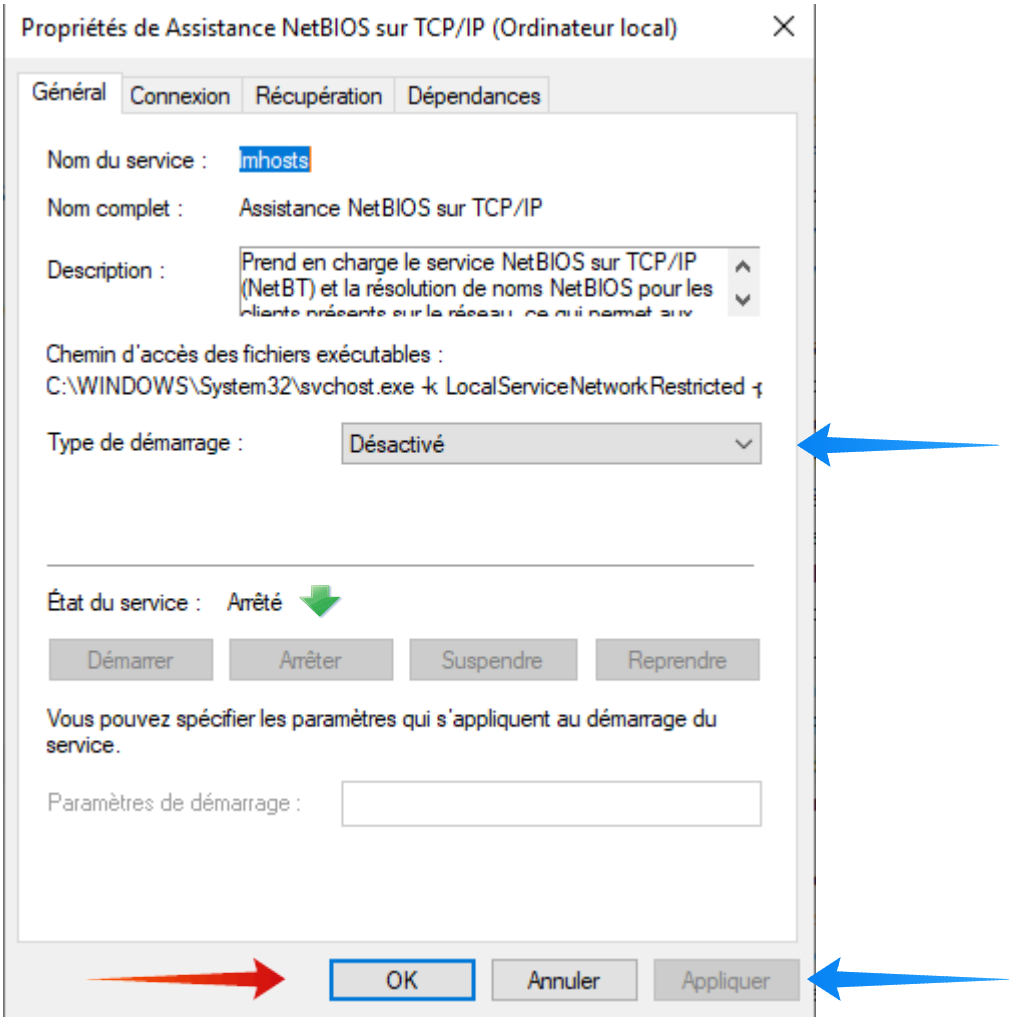
Il est souhaitable de désactiver les services Windows dangereux comme :
- Assistance Netbios sur TCP/IP,
- Configuration des services bureau à distance,
- Gestion à distance de Windows,
- Registre à distance,
- Services Bureau à distance,
- Telnet,
- Partage de connexion Internet (ICS),
- Découverte SSDP (port 1900), Hôte de périphérique UPnP (port 5000) [16];
- Service Partage réseau du Lecteur Windows Media ;
- Service SNMP pour Windows 7 & 8 (retiré de W 10 depuis Windows 10 1809), [17] ; etc... ;

ou les services dont vous n'avez peut-être pas l'utilisation : services pour la carte à puce, le Bluetooth, la WiFi, etc...

Attention de ne pas désactiver des services indispensables au bon fonctionnement de Windows : les conseils de [9], [10] et [11] sont d'une aide certaine ; par ailleurs,

certaines mises à jour de Windows réactivant malencontreusement certains services , conservez la liste des services que vous avez désactivés qui pourra, si nécessaire, vous être utile afin de rétablir les désactivations que vous aviez retenues.

Pour gérer les services dans Windows 10 :
- entrez « Services » dans la barre de recherche du menu démarrer ; dans meilleur résultat apparaît « Services, Application de bureau », faire un clic droit et choisir « Exécuter en tant qu'administrateur » ;
- dans la fenêtre des services qui s'ouvre, cliquer double sur le service à modifier ;
- dans la fenêtre « Propriétés » du service concerné qui s'ouvre : *pour désactiver le service, choisissez « Arrêter » ;*
- *puis, en face de « Type de démarrage », choisissez « Désactivé » ;*
- *puis cliquer sur les onglets « Appliquer » puis « OK »*



Annexe C – Désactiver SMBv1

SMBv1 comporte une grave faille de sécurité : Microsoft explique que SMBv1 peut (et doit) être désactivé manuellement : ouvrir le panneau de configuration ; choisir « Désactiver les fonctionnalités de Windows » ; dans la liste chercher « SMB1.0 CFS File Sharing » et décocher l'ensemble des cases.

Annexe D - Gestion des options de confidentialité

- Dans « Paramètres Windows/Confidentialité », vous avez intérêt à désactiver les options et paramètres qui ne vous sont pas nécessaires ;

- Le logiciel « O&O Shut Up 10 » peut être d'une aide précieuse dans la gestion des paramètres de confidentialité : https://www.oo-software.com/fr/shutup10

Bibliographie

[1] Dumontet Michel « **Tutoriel de COMODO Firewall et de COMODO Internet Security - 1/ Installation et configuration** », Ed. 04, 62 p. , Forum français de Comodo, septembre 2020.

https://forums.comodo.com/francais-french/tutoriel-firewall-internet-security-1-installation-configuration-securisee-t122455.0.html

[2] « **Comodo Internet Security, version 12.2** », (manuel de l'utilisateur en anglais) ;

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

https://help.comodo.com/topic-72-1-766-9024-Introduction-to-Comodo-Internet-Security.html

[3] **« 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

[4] 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 ..

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

- pour débuter l'étude de TCP/IP, malheureusement peu développé sur la sécurité, à compléter par l'ouvrage suivant ;

[6] 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 ;

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

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

- un ouvrage de référence, mais malheureusement, comme pour le précédent, il n'y-a pas d'édition plus récente ;

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

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

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

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

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

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

[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] Blocage des connexions pour les applications Windows

https://www.malekal.com/firewall-windows-les-bon-reglages/

[15] Partager un dossier entre applcations Windows

https://www.malekal.com/partager-dossier-ordinateur-windows/

[16] pour SSDP 1900 et 5000

https://www.zebulon.fr/dossiers/securite/30-securite-pc.html/6/

[17] pour SNMP

https://support.microsoft.com/fr-fr/help/324263/how-to-configure-the-simple-network-management-protocol-snmp-service-i