

Configurer son firewall : kerio

Date de dernière mise à jour : 19/07/2007 à 19:31

Source : <http://www.vulgarisation-informatique.com/kerio.php>.

Distribution interdite sans accord écrit d'Anthony ROSSETTO (<http://www.vulgarisation-informatique.com/contact.php>)

Kerio personnel firewall est un firewall en français. Il dispose d'une interface claire et simple à appréhender.

Vous pouvez commencer par télécharger kerio [ici](#). Sélectionnez **anglais** pour la langue d'installation, et installez kerio. Redémarrez ensuite votre PC.

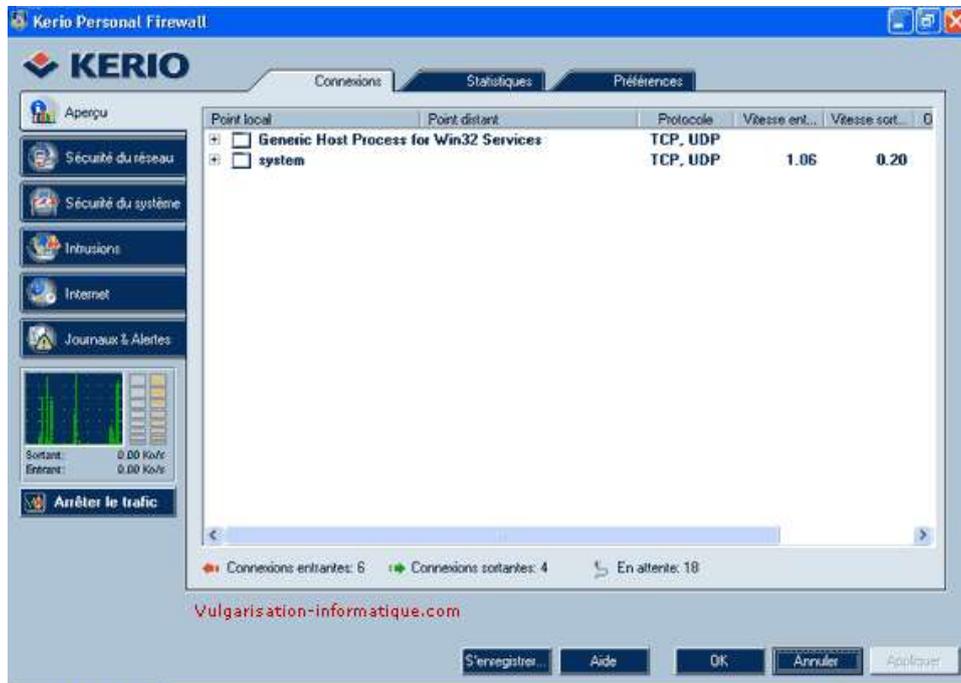
Une icône est ensuite visible dans le systray (à côté de l'horloge) :



Faites un clic droit sur cette icône, le menu permettant de configurer kerio s'affiche :



Cliquez sur **configuration**. Vous avez alors accès à toutes les options disponibles. L'écran d'accueil de kerio se présente sous cette forme :



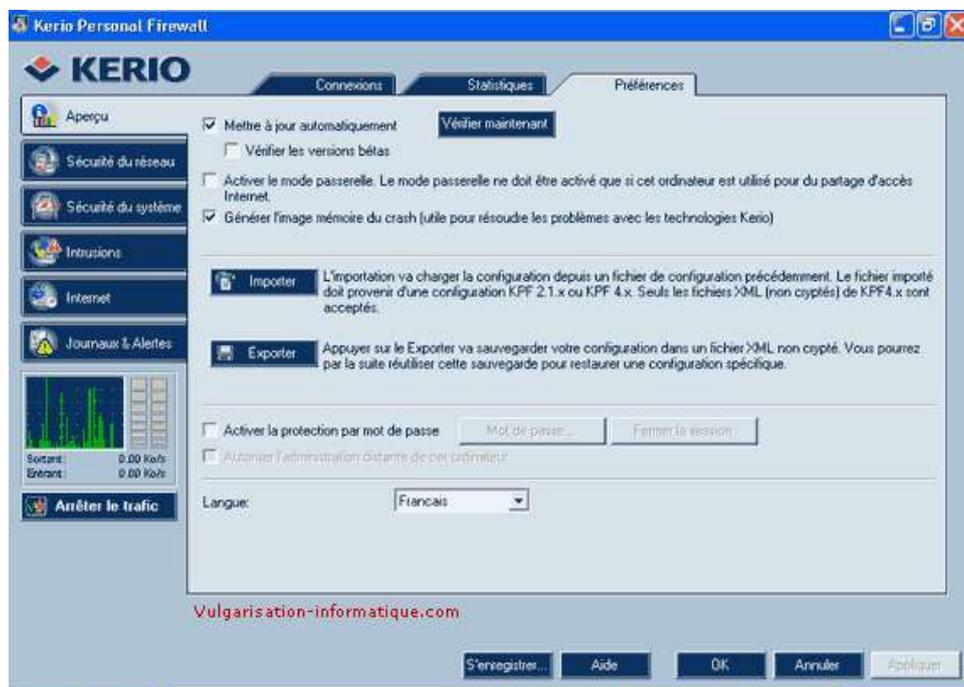
Cliquez sur un élément (ici **system**) pour afficher la liste des connexions entrantes et sortantes ainsi que les ports associés à ces connexions.



Cliquez sur l'onglet **statistiques**. Ici, en cliquant sur le groupe de statistiques que vous souhaitez consulter (par exemple **publicités**), toutes les actions modifiées ou bloquées par kerio s'afficheront sous forme de liste.

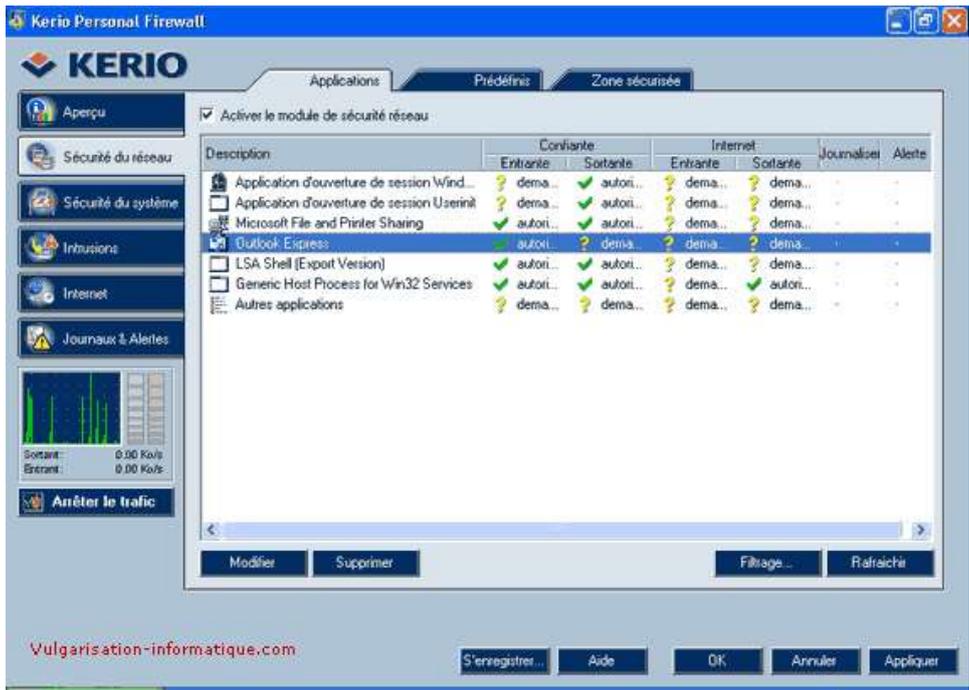


Cliquez ensuite sur l'onglet **préférences**. Vous pouvez ici configurer les options de base du logiciel. Cochez la case **Mettre à jour automatiquement** et décochez celle nommée **Vérifier les versions Beta**. Si vous souhaitez protéger la configuration de votre firewall, cochez la case **Activer la protection par mot de passe**.



Cliquez ensuite sur **Sécurité du réseau**. Les choses un peu plus sérieuses commencent. Cochez tout d'abord la case **Activer le module de sécurité**

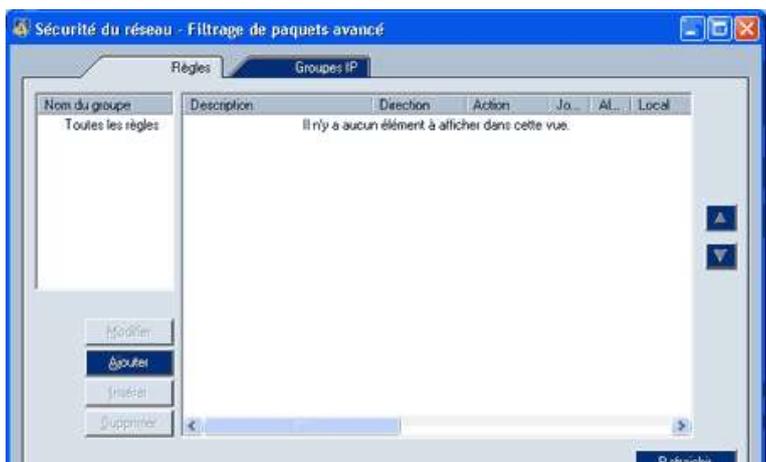
réseau. Vous pouvez ici pour chaque application listée (ou toutes les autres en cliquant sur **autres applications**) refuser sa communication localement ou à travers internet.



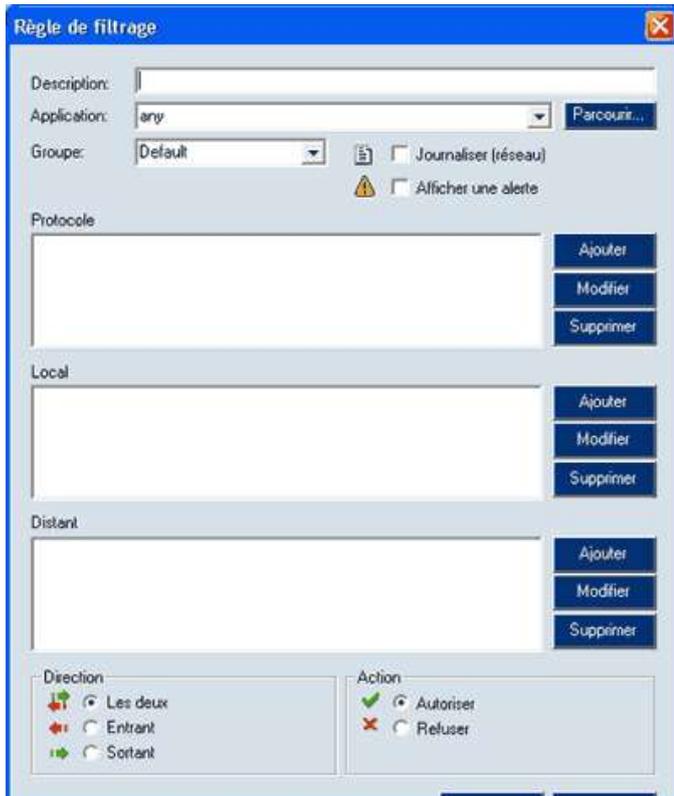
Pour modifier les droits de communication de l'application de votre choix, double cliquez sur sa description. Une fenêtre de ce type s'affiche :



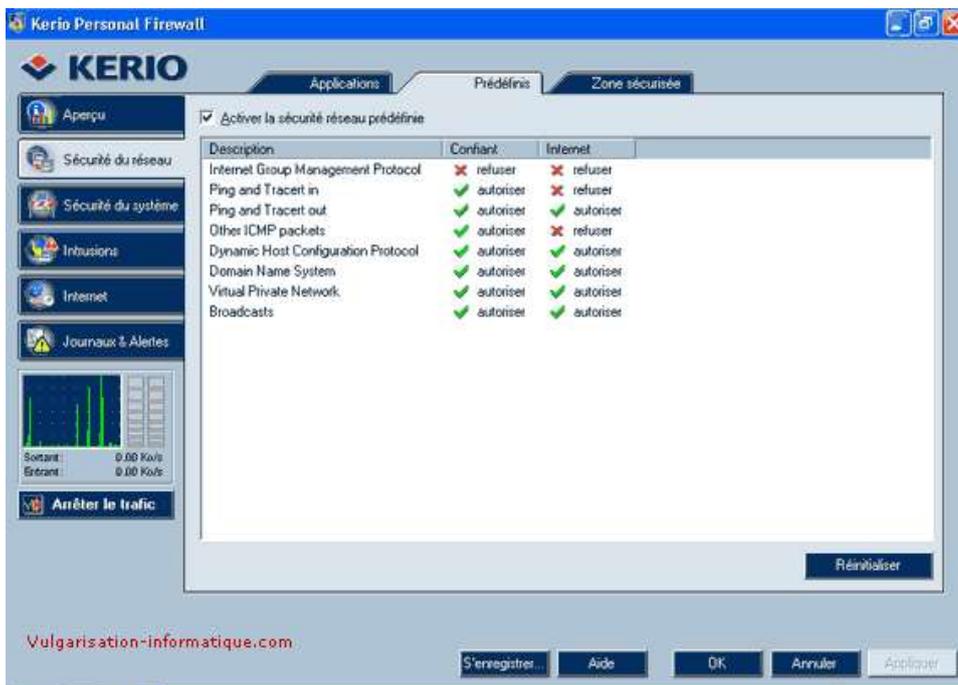
Modifiez les paramètres en fonction de la sécurité que vous souhaitez apporter. Pour un navigateur web, vous pouvez par exemple dans le cadre **Connexion depuis/vers la zone sécurisée** autoriser les connexions sortantes et refuser les connexions entrantes, de même pour internet. Une fois les paramètres modifiés cliquez sur **Ok**. Pour définir des règles de filtrage plus précises, cliquez ensuite sur le bouton **filtrage**. Les règles de filtrage s'affichent. Pour ajouter une règle de filtrage, cliquez sur **ajouter**.



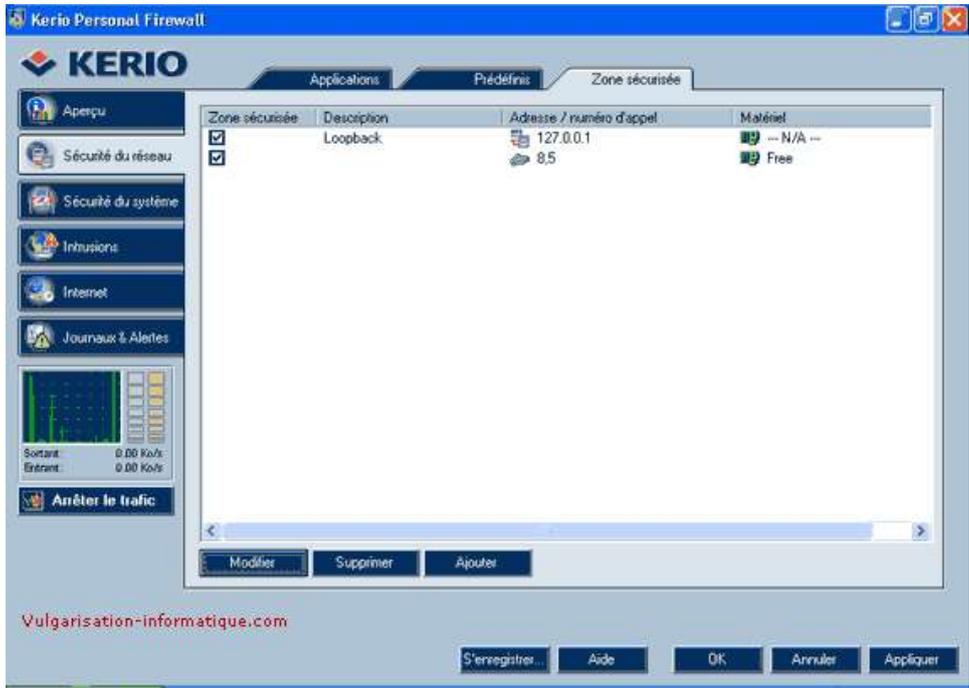
Une fenêtre de ce type s'affiche. Renseignez tout d'abord une description de la règle de filtrage, puis sélectionnez l'application pour laquelle elle doit s'appliquer. Si vous souhaitez que cette règle s'applique à toutes les applications, sélectionnez **Any**. Cliquez ensuite dans la zone **protocole** sur **ajouter** puis définissez le protocole pour lequel cette règle doit s'appliquer. Cliquez ensuite dans la zone **local** sur **ajouter** et ajoutez un port (80 par exemple pour le protocole HTTP) ou une plage de ports. Faites de même dans la zone **distant** (vous pouvez aussi ajouter une adresse IP ou une plage d'adresses IP).



Sélectionnez ensuite la direction du trafic pour laquelle cette règle doit s'appliquer et ce qu'elle doit faire (refuser ou autoriser le trafic). Cliquez ensuite sur Ok. Cliquez ensuite sur l'onglet **prédéfinis** du menu **sécurité du réseau**. Vous pouvez ici refuser ou autoriser des commandes telles que **ping**, **tracert**...



Cliquez ensuite sur l'onglet **zone sécurisée**. Vous pouvez donner ici des zones que Kerio considèrera comme étant sécurisées. Lorsque vous choisirez d'attribuer ou non des autorisations dans la colonne **Confiante** de l'onglet **Sécurité du réseau** pour diverses applications (car vous avez deux deux colonnes principales : **Confiante** et **Internet**), ces modifications prendront effet sur les zones que vous considèrerez comme sécurisées (hors connexion internet qui a une colonne pour elle). Lorsqu'une zone n'est pas considérée comme sécurisée par vous, les autorisations de la colonne **Internet** s'appliquent sur elle.



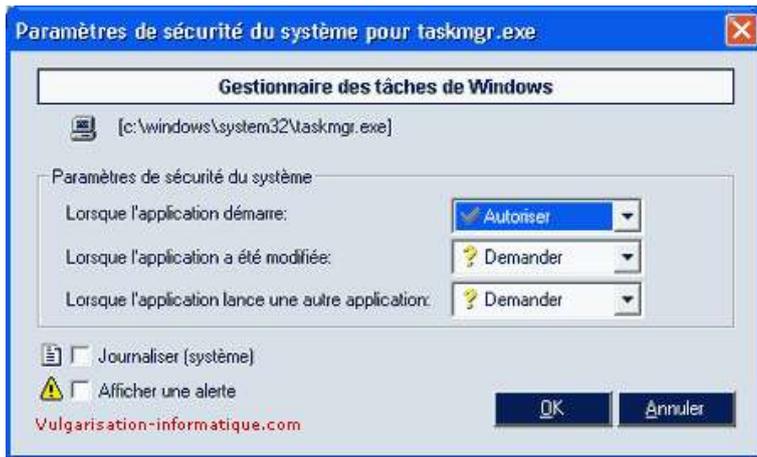
Pour ajouter une zone sécurisée, cliquez sur le bouton **ajouter**. Une fenêtre semblable à celle-ci s'ouvre :



Ajoutez une description pour votre règle, sélectionnez **tous** pour le type de matériel. Dans la zone **type d'adresse**, sélectionnez une adresse ip ou une plage d'adresses ip. Cliquez ensuite sur **ok**, puis sur l'onglet **sécurité du système**.



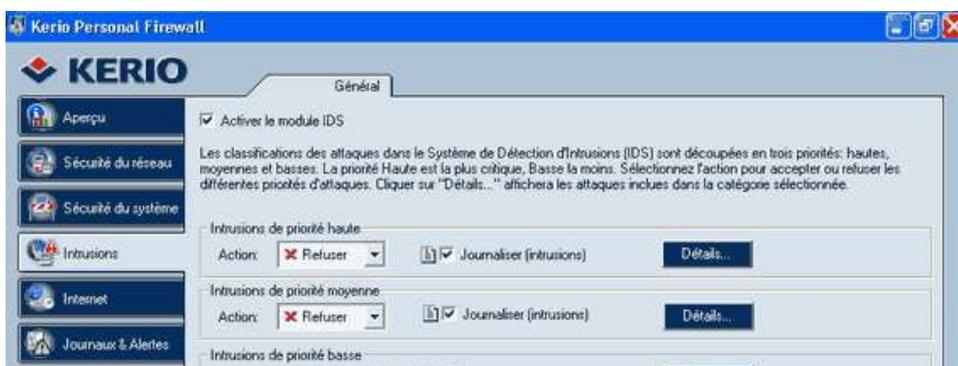
Vous pouvez ici contrôler l'exécution des applications de votre PC. Double-cliquez sur l'application dont vous souhaitez modifier les droits. Vous arrivez face à une fenêtre de ce type :



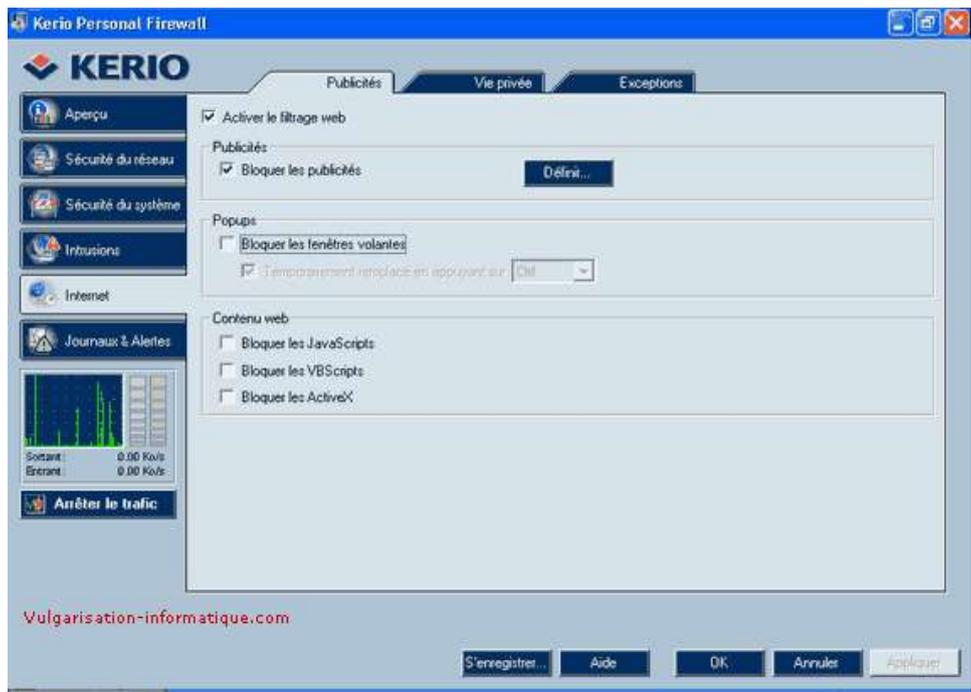
Modifiez ensuite les paramètres de l'application. Mettre **refuser** dans la zone **lorsque l'application démarre** empêchera l'application de démarrer. Cliquez ensuite sur **Ok**, puis sur l'onglet **paramètres**.



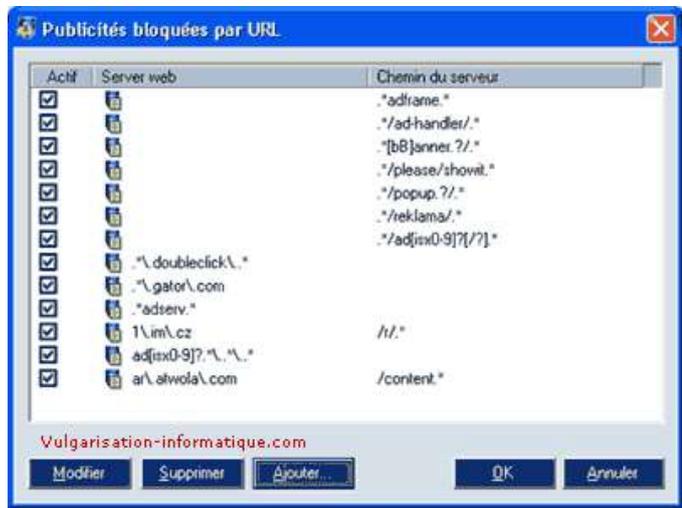
Pour un maximum de sécurité, sélectionnez pour la zone **Lorsque l'application est sur le point de démarrer**, l'option **Utiliser les règles de sécurité du système ou me demander**, de même pour la zone **Lorsque l'application est sur le point de lancer une autre application**. Cliquez ensuite sur l'onglet **intrusions**. Vous arrivez face à une fenêtre de ce type :



Mettez **Refuser** pour toutes les catégories d'intrusions, et cliquez ensuite sur l'onglet **internet**. Vous arrivez face à cet onglet :



Pour activer la protection web, cochez la case **activer le filtrage web**. Si vous cochez la case **bloquer les publicités**, vous pouvez ajouter des règles de blocage en cliquant sur le bouton **ajouter**. Vous pouvez aussi désactiver les règles initialement présentes.



Le filtrage se base sur des caractères spéciaux ou des expressions régulières. Si vous pensez que les caractères spéciaux ne sont pas assez puissants pour définir la règle de filtrage que vous souhaitez, cochez la case **utiliser les expressions régulières au lieu des caractères spéciaux**. Une fois votre règle définie, cliquez sur **ok**.



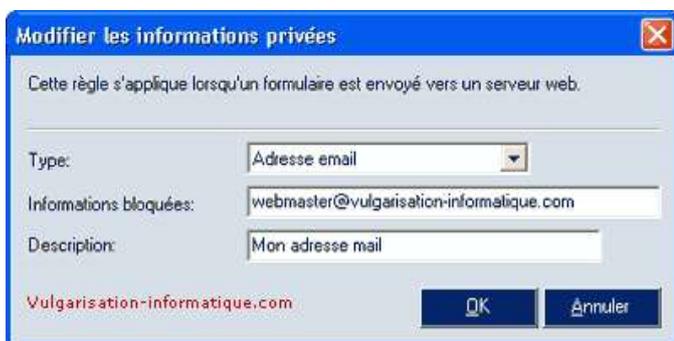
Cliquez ensuite sur l'onglet **vie privée** et cochez la case **filtrer les cookies étrangers**. Vous pouvez également cocher la case **refuser aux serveurs de tracer la navigation**. Cochez la case **bloquer les informations privées** et cliquez sur **définir**.



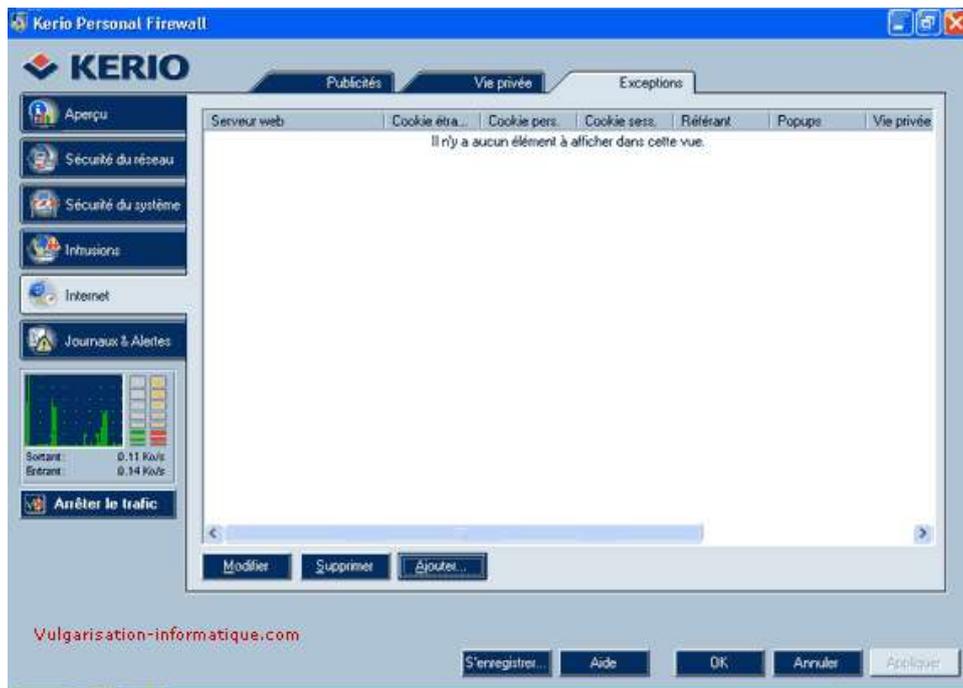
Vous arrivez face à un écran de ce type. Pour ajouter une information privée à bloquer, cliquez sur **ajouter**.



Vous pouvez alors choisir le type d'information à bloquer dans cette fenêtre. Une fois votre règle établie, cliquez sur **ok**.



Cliquez ensuite sur l'onglet **exceptions**. Vous pouvez configurer ici des adresses web pour lesquelles vous pouvez définir des règles personnalisées.



Pour ajouter une règle, cliquez sur le bouton **ajouter**. Une fenêtre semblable à celle-ci s'ouvre :

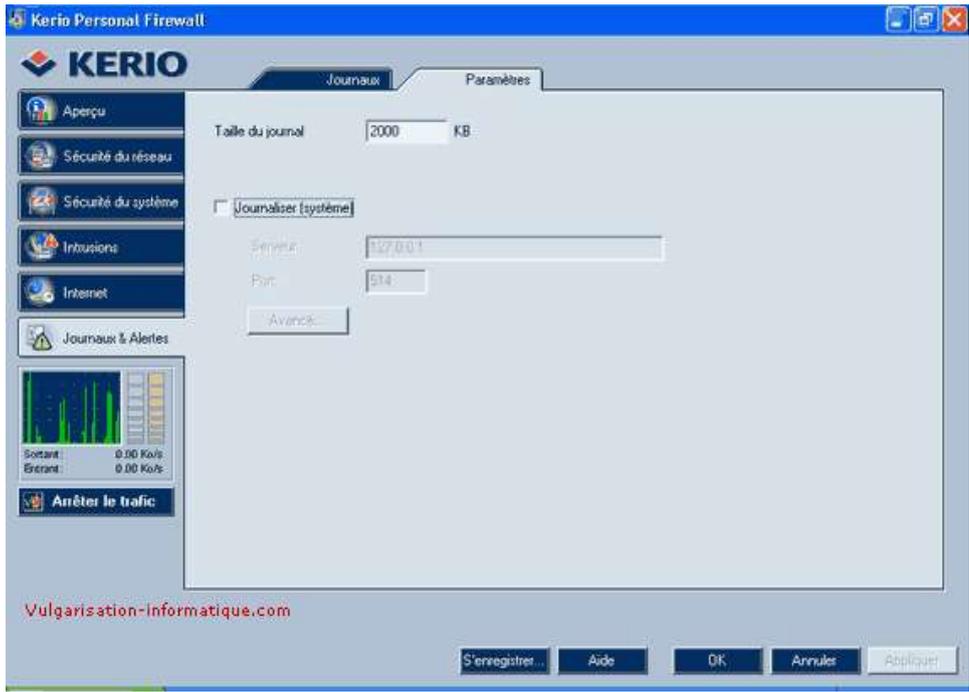


Le principe est le même : caractères spéciaux ou expressions régulières. Une fois l'adresse du site inscrite, cliquez sur **blocage** et ensuite sur **vie privée** pour configurer les paramètres comme si vous le faisiez globalement (vu précédemment)

Cliquez ensuite sur l'onglet **journaux et alertes**. Vous pouvez consulter ici toutes les alertes et autres blocages effectués par Kerio.



Cliquez sur l'onglet **paramètres** pour configurer la taille maximale du journal. Indiquer dans la case **taille du journal** une valeur de 2048 pour 2 Mo est une valeur correcte. Si vous souhaitez enregistrer les logs sur un serveur distant (ou local), cochez la case **journaliser (système)** et indiquez l'adresse ip et le port (par défaut 514) associé. Vous pouvez ensuite configurer ce qui est à journaliser en cliquant sur le bouton **avancé**.



Lorsque Kerio vous alerte, vous avez des écrans de ce type :



Vous pouvez alors cocher la case **créer une règle pour cette communication et ne plus me demander** pour ne plus recevoir d'alerte.

Source : <http://www.vulgarisation-informatique.com/kerio.php>.

Distribution interdite sans accord écrit d'Anthony ROSSETTO (<http://www.vulgarisation-informatique.com/contact.php>)