**Mise en place d’une liste noire et mise à jour pour ISA Server 2004**

**Sommaire**

**La liste noire**

**Besoin**

**Mise en oeuvre**

**Stratégie pour récupérer la blacklist**

**Interdiction d’accès aux sites de la liste**

**Test et interprétatino du log**

**Mise en œuvre la MAJ auto**

Cet article décrit comment bloquer l’accès à des sites à caractère pornographique avec ISA Server 2004 à l’aide d’une liste noire (blacklist)

# Qu’est ce que c’est une liste noire

Une liste noire (« blacklist ») est une liste d’adresses Internet qui a été jugée par une autorité comme destructive d’un point de vu ou d’un autre. Dans notre cas, cette blacklist va contenir une série de sites et domaines avec caractère pornographique.

**Besoins**

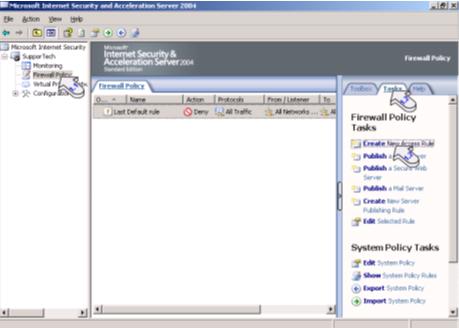
Dans cet article, vous allez voir comment mettre en place une blacklist basée sur le serveur ISA Server 2004. L’outil Winrar a été choisi pour désarchiver la blacklist une fois qu’elle est téléchargée depuis l’Internet. A la fin de la mise on œuvre, le serveur ISA interdira l’accès depuis l’intérieur de votre établissement vers les sites (avec un caractère pornographique) déclares dans cette liste.

**Mise en œuvre de la liste noire**

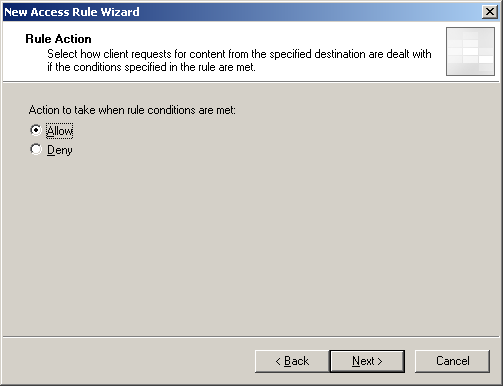
## Stratégie pour récupérer la blacklist

Il est ici être question de la création d’une stratégie permettant au serveur ISA de se connecter sur Internet et de récupérer la blacklist du serveur FTP de Toulouse. Il est à noter que le serveur ISA utilisé est en langue Anglaise.

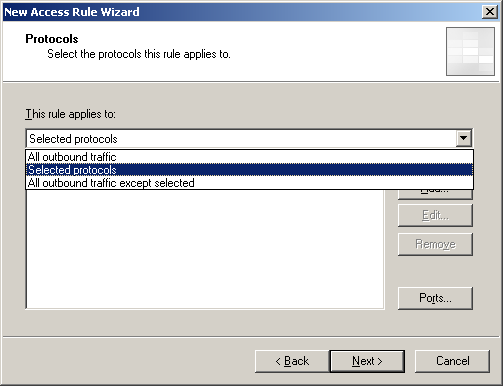
1. Dans la console d’administration du serveur ISA, choisissez « Firewall Policy » dans la branche avec le nom du votre serveur ISA
2. Dans l’onglet « Tasks » du menu à droite, créez une nouvelle règle en cliquant sur « Create New Access Rule »



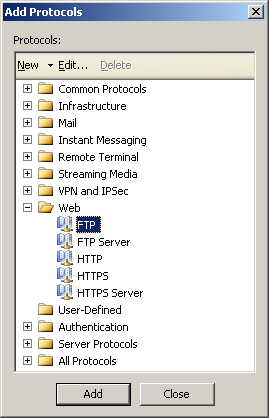
1. Donnez le nom « Accès ISA au FTP Blacklist » à cette règle, puis cliquez sur « Next »
2. Sélectionnez « Allow » dans la fenêtre « Rule Action », puis cliquez sur « Next »



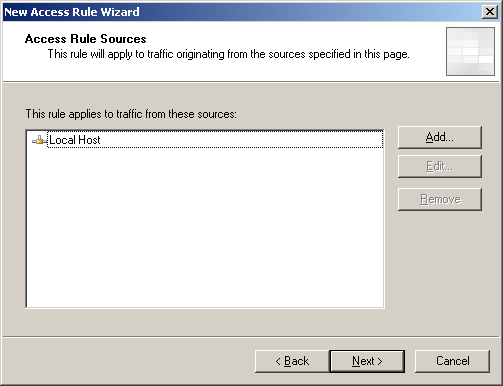
1. Dans la fenêtre « Protocols », au lieu de « All outbound traffic », choisissez « Selected Protocol »



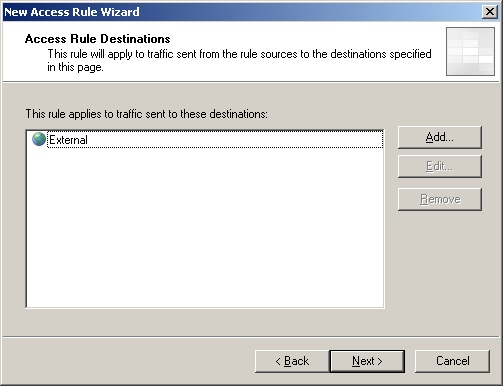
1. Ajoutez le protocole « FTP » qui se trouve dans la branche « Web », puis cliquez sur « Close » et « Next »



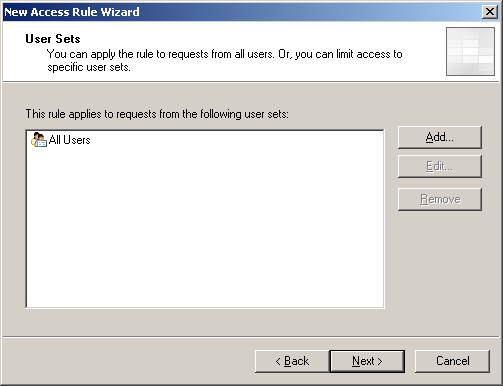
1. Dans la fenêtre « Access Rule Sources », ajoutez la source « Local Host » (qui est équivalent au serveur ISA). Vous trouvez « Local Host » dans la branche « Networks »



1. Dans la fenêtre « *Access Rule Destinations »*, ajoutez « *External »*, que vous allez trouver dans la branche « *Networks »*



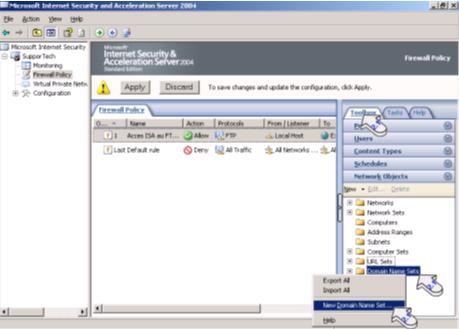
1. Dans la fenêtre « User Set »s laissez l’objet « All Users » qui est mis par défaut, puis cliquez sur « Next » et « Finish »

**

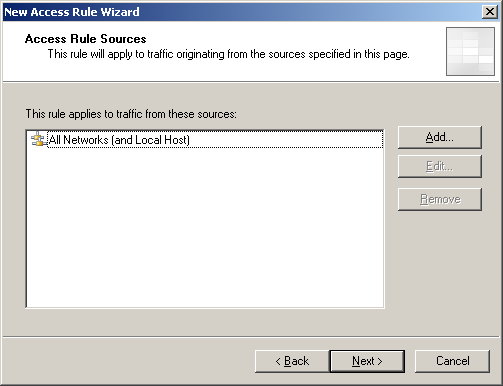
## Stratégie d’interdiction d’accès aux sites présents dans la liste noire

Ici, on va créer une stratégie interdisant l’accès depuis l’intérieur du réseau sur des sites qui sont dans la blacklist.

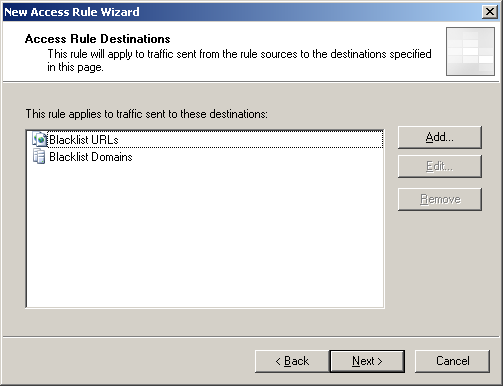
1. Dans l’onglet « Toolbox » du menu à droite, faites clique droit sur « Domain Name Sets », puis cliquez sur « New Domain Set »



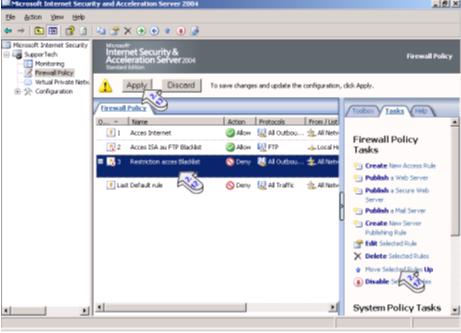
1. Donnez le nom « Blacklist Domains » à cet ensemble de domaines, puis cliquez sur « OK »
2. Dans l’onglet « Toolbox » du menu à droite, faites clique droit sur « URL Sets », puis cliquez sur « New URL Set »
3. Donnez le nom « Blacklist URLs » à cet ensemble de URL, puis cliquez sur « OK »
4. Dans l’onglet « Tasks » du menu à droite, créez une nouvelle règle en cliquant sur « Create New Access Rule »
5. Donnez le nom « Restriction accès Blacklist » à cette règle, puis cliquez sur « Next »
6. Sélectionnez « Deny » dans la fenêtre « Rule Action », puis cliquez sur « Next »
7. Dans la fenêtre « Protocols », laissez le paramétrage par défaut « All outbound traffic »
8. Dans la fenêtre « Access Rule Sources », ajoutez « All Newtorks (and Local Host) » qui se trouve dans la branche « Network Sets »



1. Dans la fenêtre « Access Rule Destinations », ajoutez les destinations « Blacklist Domains » et « Blacklist URLs », que vous allez trouvez dans la branche « Domains Name Sets » et respectivement « URL Sets ».



1. Dans la fenêtre « User Sets » laissez l’objet « All Users » qui est mis par défaut, puis cliquez sur « Next » et « Finish »
2. Assurez vous que la règle d’interdiction d’accès sur les sites de la blacklist est évaluée avant celle qui donne accès Internet à vos utilisateurs. Pour cela, sélectionnez la règle, et cliquez sur « Move Selected Rules Up » dans le menu a droite
3. À la fin, appliquez toutes les changements en cliquant sur le bouton « Apply » sur la barre en haut



# Test et interprétation du log

Le script exécute plusieurs actions :

1. Effacement des fichiers utilisés pendant la mise à jour précédente
2. Téléchargement de la blacklist
3. Décompression de la liste
4. Transformation de la liste de domaines au format xml
5. Transformation de la liste d'url au format xml
6. Importation de la liste d'url dans ISA
7. Importation de la liste de domaines dans ISA

Avant que le script n'exécute chacune de ces actions, le nom de l’action ainsi que l'heure et la date du système sont écrites dans le fichier de log « *C:\blacklist.log »*. Lorsque la taille du fichier « *blacklist.log »* dépasse 2 Mo, ce fichier est copié dans « *blacklist.log.old »* et un nouveau fichier « *blacklist.log »* est créé.

Dans un premier temps, on essayera d’exécuter le script depuis la ligne de commande, afin de vérifier que toutes les manipulations ont été correctement réalisées. Pour cela, copiez le contenu de l’archive dans le répertoire « *C:\blacklis »t*. Dans ce répertoire il faut copier l’utilitaire « *Winrar.exe »* et le sous répertoire « *Formats »*, que vous allez trouver dans « *C:\Program Files\WinRar »*

Une fois que cette manipulation à été effectué, rendez-vous dans une console (*Start,* *Run, cmd*) et exécutez « c*d \Blacklist »* puis « *Blacklist »*

Vous pouvez voir maintenant les actions que sont effectuées par le script en temps réel.

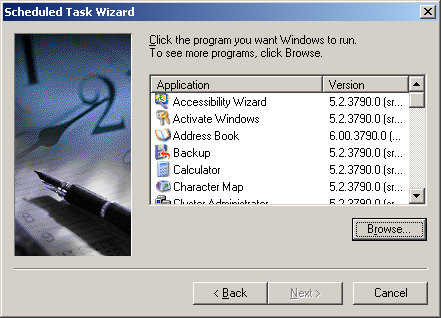
Parmi les actions du script, les parties 6 et 7 peuvent prendre quelques minutes à s’exécuter en fonction de la puissance de votre machine. Elles sont associées aux commandes « *populateurls.vbs »* et « *populatedomains.vbs* » du fichier « *Blacklist.bat »*.

Si le script a été exécuté avec succès et vous n’avez pas eu d’avertissements, vous pouvez passer à l’étape suivante.

# Mise on œuvre de la mise à jour automatique

Maintenant que vous avez la blacklist active sur votre serveur ISA, il est temps de la configurer de sorte qu’elle se mette à jour régulièrement et automatiquement.

Dans *Start, Programs, System Tool*s, *Scheduled Tasks* cliquez sur « *Add Scheduled Task”*. Une fois le nom de la tâche demandé, cliquez sur « *Browse »*



Puis indiquez le fichier « *Blacklist.bat »* du répertoire « *C:\blacklist* »



Mettez l’intervalle de temps à « Daily*»* et le temps d’exécution à « *03:00 AM »*. A la fin, utilisez un compte d’utilisateur qui a des droits d’administration pour le lancement de la tache planifié.