

Mise en œuvre: administration

10 mesures
pour améliorer l'efficacité
de Microsoft Proxy Server 2.0

Patrick CHAMBET
<http://www.chambet.com>

L'objectif de cet article:

Améliorer les performances et la sécurité de votre réseau en apprenant comment administrer efficacement MS Proxy Server 2.0.

Les outils utilisés:

- Microsoft Proxy Server 2.0
- Le serveur Web Microsoft IIS 4.0
- La MMC (Microsoft Management Console) d'IIS 4.0

Pour en savoir plus:

- http://www.microsoft.com/products/prodref/590_ov.htm Product Overview
- <http://www.microsoft.com/proxy> MS Proxy Server Web Site
- <http://www.microsoft.com/proxy/guide/Security.asp> MS Proxy Server White Paper
- <http://proxyfaq.networkgods.com> Un site bourré d'informations sur Proxy Server
- Articles de la Knowledge Base de Microsoft:
 - <http://support.microsoft.com/support/kb/articles/Q174/9/22.asp> (Release Notes de Proxy Server)
 - <http://support.microsoft.com/support/kb/articles/Q176/7/71.asp> (Utilisation du filtrage de paquets avec un serveur Exchange)
 - <http://support.microsoft.com/support/kb/articles/Q181/4/20.asp> (Configuration d'un serveur mail avec Proxy Server)
 - <http://support.microsoft.com/support/kb/articles/Q185/6/38.asp> (Configuration de SQL Server avec Proxy Server)
 - <http://support.microsoft.com/support/kb/articles/Q177/1/53.asp> (Autres configurations avec Proxy Server)
 - <http://support.microsoft.com/support/kb/articles/Q178/1/73.asp> (Bug: Proxy Server peut ne pas interpréter certains scripts correctement)
 - <http://support.microsoft.com/support/kb/articles/Q183/2/83.asp> (Bug: le contrôle d'accès peut provoquer un retour de page blanche)
 - <http://support.microsoft.com/support/kb/articles/Q177/9/06.asp> (Le caching ne fonctionne pas en Reverse-Proxying)

A quoi sert Proxy Server 2.0 de Microsoft ? Est-il une bonne solution de sécurité ? Ces questions, souvent posées, reflètent la difficulté de positionnement de ce produit.

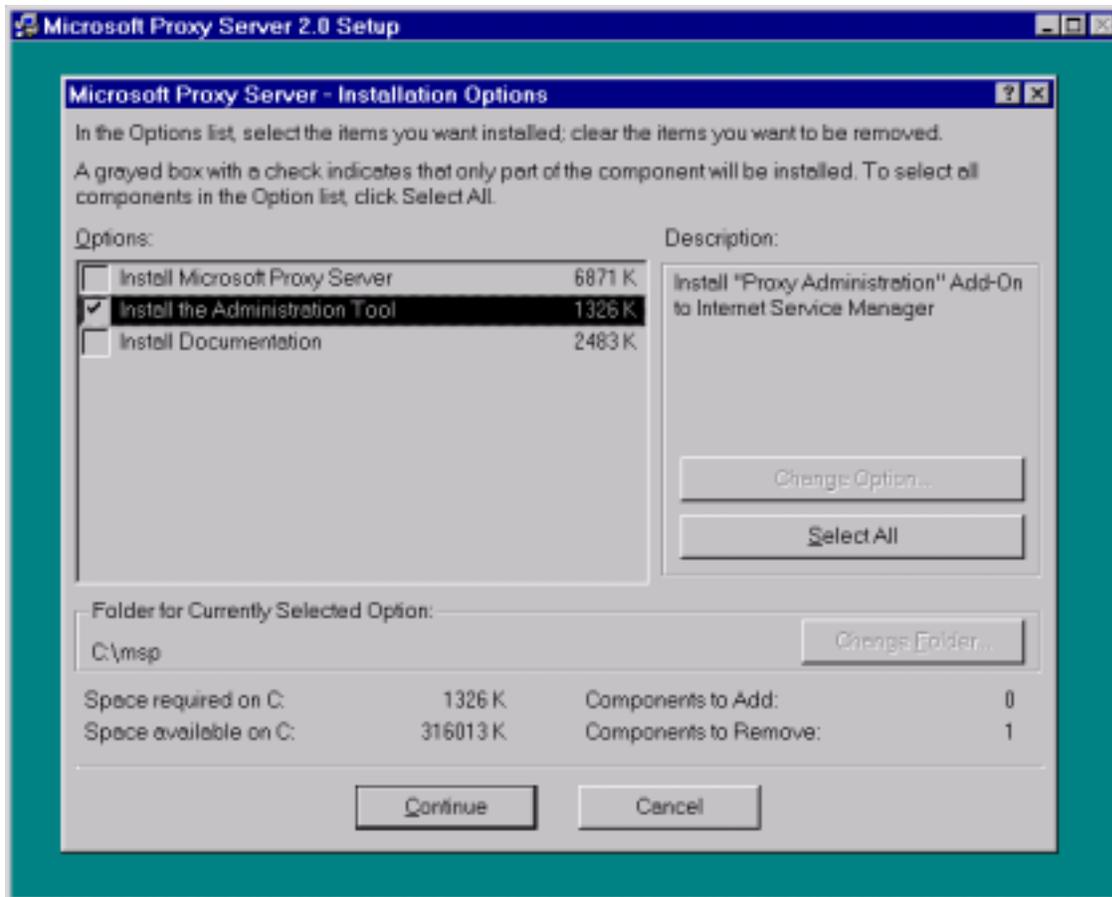
Microsoft Proxy Server est un serveur Proxy possédant en plus certaines fonctions de Firewall. Soyons clair: ce n'est **pas** un Firewall, et il ne doit pas être utilisé seul pour protéger un site dont la sécurité doit être élevée.

Cela dit, il offre tout de même des fonctions de sécurisation importantes, comme le filtrage de paquets dynamique.

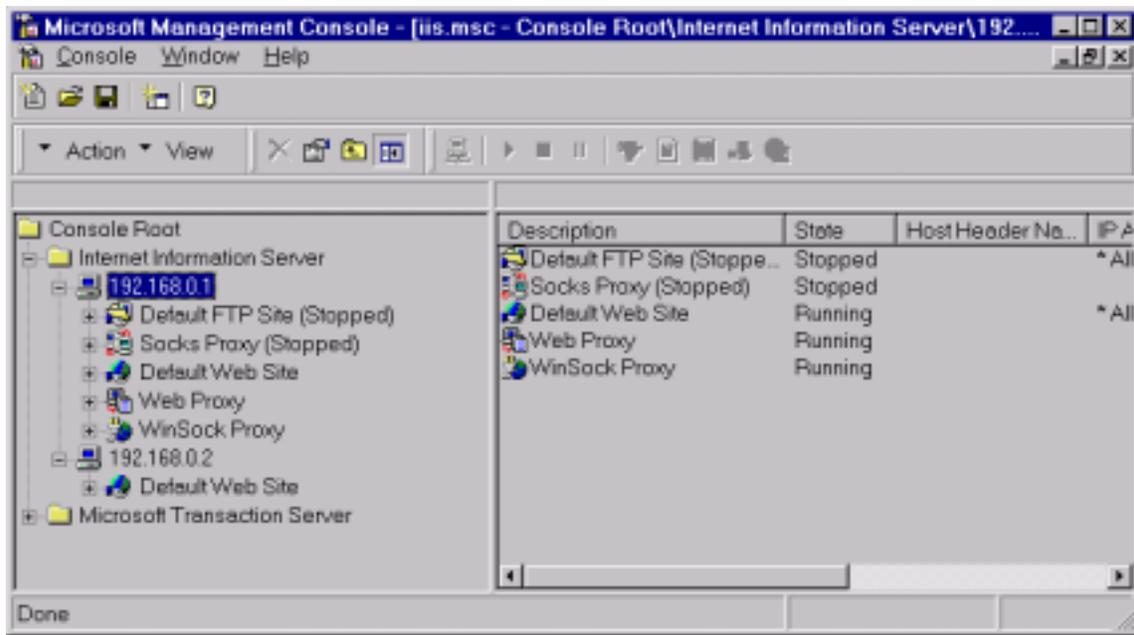
Du fait de ses fonctions avancées, MS Proxy Server 2.0 peut paraître difficile à administrer de prime abord. Cet article ne se veut pas une prise en main pour débutant, mais un recueil de méthodes pour administrer plus efficacement MS Proxy Server 2.0

1 - ADMINISTRER MS PROXY SERVER A DISTANCE

Vous pouvez administrer MS Proxy Server depuis n'importe quelle station de travail de votre réseau sur laquelle la MMC est installée. Il suffit d'installer les outils d'administration sur cette station. Pour cela, lancez le Setup de MS Proxy Server et cochez uniquement le deuxième choix:



Vous avez maintenant accès, dans le snap-in Internet Information Server, aux paramètres des Proxies Web, Winsock et Socks:



CONFIGURATIONS DE BASE

2 - Permissions NTFS

Il faut faire attention aux permissions NTFS accordées sur les répertoires suivants:

\Inetpub\Scripts\Proxy
 \Urlcache

En effet, il faut que les utilisateurs de Proxy Server aient les droits "Read/Execute" ou "Full Control" sur ces répertoires ainsi que sur leurs sous-répertoires. Il faut aussi que le compte "System" aie les droits "Full Control" sur ces répertoires. A défaut, des erreurs d'authentification peuvent apparaître (cf article Q177502).

3 - Adresses IP multiples sur la carte externe

Si vous affectez plusieurs adresses IP à une seule carte réseau externe, n'activez pas le filtrage de paquets dynamique. En effet, dans ce cas, le filtrage de paquets ne réussira pas à se lancer.

Mais MS Proxy Server supporte jusqu'à 3 cartes réseau externes. Vous pouvez donc éventuellement installer 3 cartes et affecter une adresse externe différente sur chacune d'elle.

Pour en savoir plus: <http://support.microsoft.com/support/kb/articles/Q176/9/22.asp>

CONFIGURATIONS AVANCEES

4 - Désactiver le proxy SOCKS

Si vous n'utilisez pas le proxy SOCKS, vous pouvez désactiver ce service pour l'empêcher de démarrer automatiquement au boot. Pour cela, il faut modifier une clé dans la base de Registres de NT.

1 - Lancez REGEDT32 ou REGEDIT et naviguez jusqu'à la clé:

```
HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/W3Proxy/Parameters/Socks
```

2 - Localisez la valeur SocksServiceEnabled

3 - Changez sa valeur de 1 (défaut) à 0.

4 - Rebootez.

Le service Socks Proxy ne démarrera plus jamais, même si vous essayez de le lancer depuis la MMC. Pour le relancer si besoin est, modifiez à nouveau la clé de la base de registre pour lui rendre sa valeur initiale.

5 - Permettre le support du FTP passif

Par défaut, MS Proxy Server ne supporte que le FTP non passif (c'est-à-dire que c'est le client qui est responsable de l'établissement de toutes les connexions avec le serveur), qui est plus sûr, car il offre une protection accrue contre une attaque en provenance d'un serveur FTP.

Mais certaines applications utilisent le FTP passif. Si vous désirez que votre Proxy Server supporte le FTP passif, il faut, là encore, modifier une clé de la base de Registres:

1 - Lancez REGEDT32 ou REGEDIT et naviguez jusqu'à la clé:

```
HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/W3Proxy/Parameters
```

2 - Localisez la valeur NonPassiveFTPTransfer

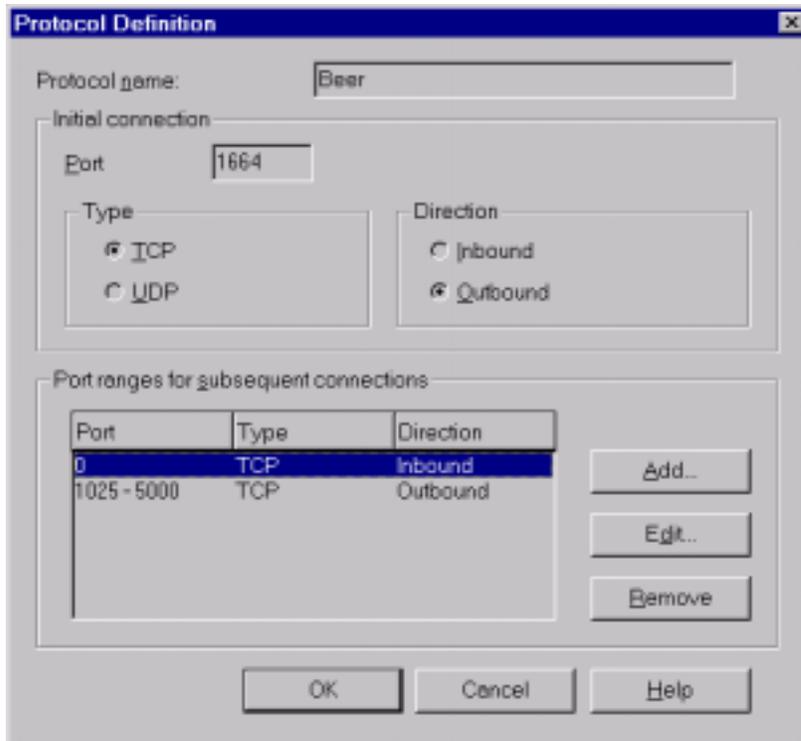
3 - Changez sa valeur de 1 (défaut) à 0.

6 - Ajouter un protocole propriétaire

Supposons que les machines de votre réseau interne aient besoin d'établir une connexion vers un serveur externe qui utilise un protocole propriétaire sur le port 1664. Vous pouvez autoriser l'établissement de ces connexions et des connexions en retour en créant votre propre protocole dans l'onglet "Protocols" des propriétés de votre Winsock Proxy. Pour cela:

1 - Cliquez sur "Add..."

2 - Paramétrez par exemple les éléments suivants:



Ces paramètres permettront donc à chaque client de votre réseau d'établir une première connexion TCP vers l'extérieur sur le port 1664, puis de recevoir les connexions TCP en retour (la valeur 0 pour le port signifie `Port_Any`, c'est-à-dire que le serveur peut choisir un port entre 1024 et 5000) et d'y répondre, toujours en TCP.

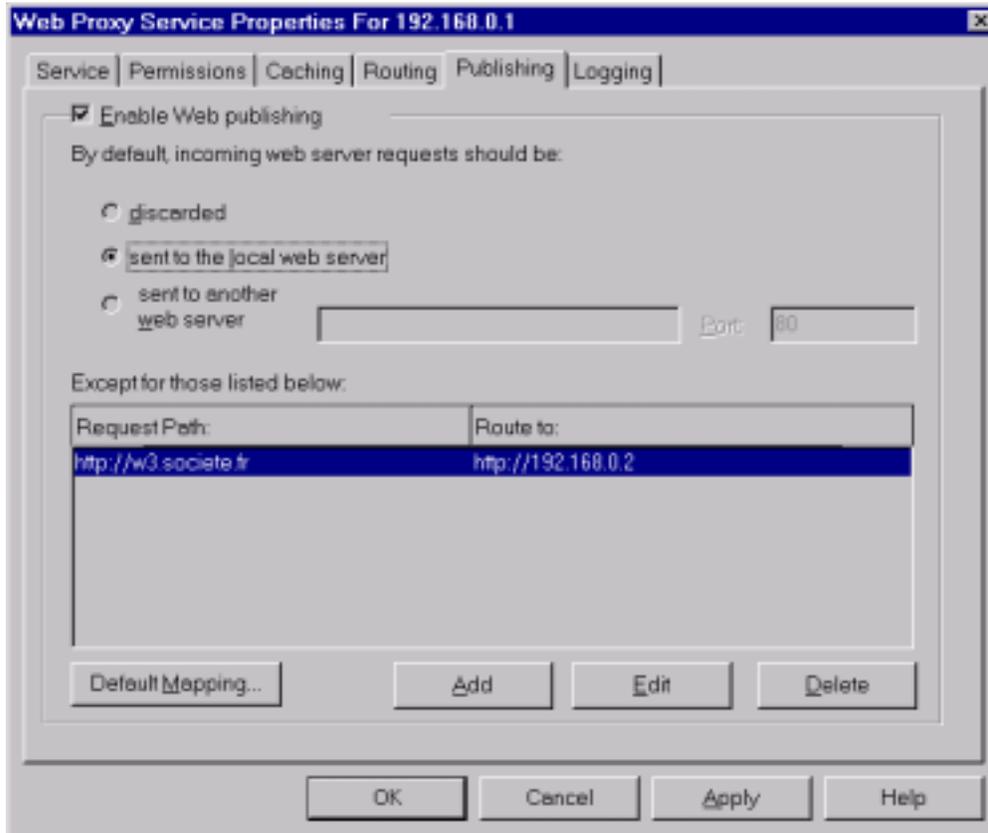
7 - Publier un serveur interne vers l'extérieur: le Reverse Proxying

MS Proxy Server offre la possibilité de publier le contenu d'un serveur Web interne vers Internet. C'est le Reverse Proxying.

L'onglet "Publishing" des propriétés du Web Proxy permet de sélectionner le traitement qui sera appliqué aux requêtes HTTP provenant de l'extérieur: soit ne pas y répondre, soit les envoyer sur le serveur IIS 4.0 local, soit les envoyer vers un autre serveur, interne par exemple. Celui-ci sera désigné de préférence par son adresse IP interne.

On peut aussi définir des exceptions. Dans l'exemple ci-dessous, toutes les requêtes HTTP arrivant sur le Proxy Server seront redirigées vers le serveur

Web local (www.societe.fr) sauf les requêtes sur <http://w3.societe.fr>, qui seront renvoyées vers le serveur interne 192.168.0.2.



Dans ce cas, le DNS gérant le domaine `societe.fr` devra comporter des enregistrements pour www.societe.fr et w3.societe.fr.

ATTENTION: le reverse proxying ne fonctionne que si l'accès anonyme est autorisé sur le Proxy ET sur le serveur Web interne !

8 - Le problème de SSL sur le réseau local

Pour permettre des connexions sécurisées par SSL avec l'extérieur, il vous faut installer un certificat SSL sur le serveur IIS hébergeant votre Proxy Server. Mais la connexion issue du reverse proxying entre le Proxy Server et le serveur Web interne, elle, ne sera pas cryptée (voir l'article Q174586).

Si la protection de vos données est importante également sur votre réseau interne, il vous faudra installer un autre certificat SSL sur votre serveur Web interne et configurer votre Proxy Server pour qu'il établisse sa connexion issue du reverse proxying en HTTPS sur le port 443.

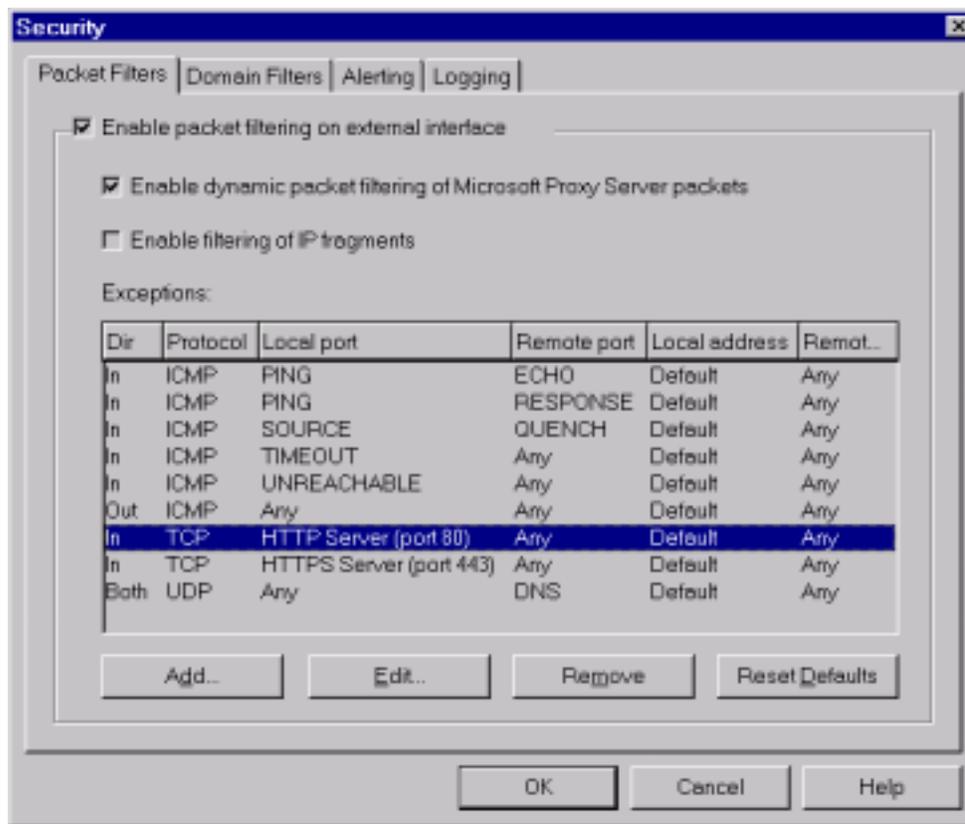
Remarque: dans ce cas, les performances seront légèrement dégradées par le fait que le Proxy Server sera contraint à un double cryptage/décryptage des requêtes HTTPS de chaque côté.

9 - Autoriser la publication sur Internet avec le filtrage de paquets activé

Si vous activez le filtrage de paquets, vous ne pouvez plus publier depuis votre réseau local vers Internet, à moins d'ajouter les filtres prédéfinis HTTP et HTTPS Server.

Pour cela, allez dans les propriétés du Web Proxy, cliquez sur le bouton "Security...", puis sur le bouton "Add..." de l'onglet "Packet Filters".

Dans la liste "Predetermined filters", choisissez les filtres **HTTP Server (port 80)** et éventuellement **HTTPS Server (port 443)**.



Remarque: l'activation du filtrage de paquets dynamique, s'il n'est pas indispensable à la sécurité du réseau, devrait être inactif. En effet, il est source de problèmes (dans la version 2.0 de MS Proxy en tout cas) et peut ralentir les échanges (avec MS Exchange, par exemple: voir l'article Q176947).

AUTRES ASTUCES

10 - Utilisez l'utilitaire de diagnostic pour le client Proxy

Quand vous installez le client Proxy sur une station de travail, de votre réseau, généralement dans le répertoire C:\mspclnt, un utilitaire de diagnostic est copié automatiquement dans ce répertoire. Sur les systèmes 32 bits, cet utilitaire se nomme Chkwsp32.exe. Sur les systèmes 16 bits, il s'agit de Chkmsp16.exe.

Pour lancer cet utilitaire, ouvrez une fenêtre de commande et déplacez vous dans le répertoire Mspclnt. Lancez l'utilitaire avec l'option -f: chkmsp32 -f
Vous obtenez les informations suivantes:

```
*****
****      Winsock Proxy Diagnostic Information      ****
*****

WAIT...

CONFIGURATION:
  Winsock Proxy Service - Configuration Location: C:\mspclnt
  Proxy Name (IP Addr):
    Addr1: 192.168.0.1 ( SERVER_NAME )
  WINSOCK 2.0: WSP is a Layered Service Provider
  IP:      Installed
  IPX:     Not Installed

WAIT...

32-bit WSP CLIENT:
  Winsock Name: C:\WINNT\System32\wsock32.dll
  Version: 4.0.1371.1
  Description: Windows Socket 32-Bit DLL
  Version Type: FREE
  Layered Service Provider version: 2.0.372.12
  Client version of control protocol: 10

WSP SERVER:
  Testing against server: 192.168.0.1 ( SERVER_NAME )
  Version: 2.0.372.12
  Version Type: FREE
  Server version of control protocol: 10
  Windows version: 4.0
  Windows build number: 1381

-----

Client control protocol version MATCHES the server control protocol
```

Pour finir, une bonne habitude à prendre est de vérifier régulièrement la publication par Microsoft de nouveau patches et fixes, pour NT, IIS 4.0 et Proxy Server 2.0. Les exécutables pour ces trois produits se trouvent respectivement aux endroits suivants:

- NT 4.0 : <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp3/> pour les Hot Fixes post-SP3 et

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp4/> pour le SP4 qui vient tout juste de sortir.

- IIS 4.0 : <ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/>

- Proxy Server 2.0 : <ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/proxy/> et <http://proxyfaq.networkgods.com/downloads.htm>

Patrick Chambet