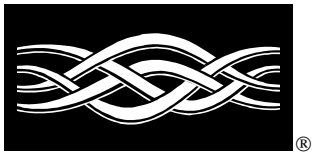


Livre Blanc

Proxy 2.0 :
Notions avancées pour le support technique

Lionel CAU, septembre 1999.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Microsoft®
BackOffice™

Abstract

Les informations recueillies dans ce document sont tirées du MSDN, d'articles techniques, d'extrait de documents du TechNet et d'Internet et d'expériences personnelles. Le but de ce livre blanc n'est pas d'exposer ou d'expliquer les fonctionnalités de Microsoft Proxy server mais d'en détailler certains points pour faciliter la résolution de problèmes inhérents à son utilisation et son support technique.

SOMMAIRE

Introduction 6

1. Installation d'un serveur 7
1.1. Rôle du serveur 7
1.2. Installation par ligne de commande 7
1.3. Installation en Unattended 7
1.4. Ne pas oublier le fichier journal d'installation ! 9
1.5. Mettre en place le SP1 9
1.6. Proxy 2.0 et Windows 2000 10

2. La connexion entre le serveur Proxy et le réseau interne 11
2.1. Le nombre de cartes réseau 11
2.2. Le protocole Netbios 11

3. La connexion entre le serveur Proxy et le réseau externe ... 13
3.1. Utilisation d'une carte réseau pour se connecter au réseau externe 13
3.2. Utilisation d'un modem 13

4. Protéger le réseau local de l'extérieur 14
4.1. Rappels sur les différentes définitions dans l'interface 14
4.2. Le filtrage de paquets 15
4.3. Le filtrage de paquets et les protocoles non gérés par les services Proxy 16
4.4. La checklist 17

5. Installation d'un client 18
5.1. Utilisation du service Web Proxy 18
5.2. Utilisation du service Socks Proxy 18
5.3. Installation du client Winsock Proxy en ligne de commande 19
5.4. Installation en Unattended 20
5.5. Ne pas oublier le fichier journal d'installation ! 20
5.6. Les fichiers du client Winsock Proxy 20

6. Utiliser le service Web Proxy 24
6.1. Configurer son browser 24
6.2. Les critères de mise en cache 6
6.3. Favoriser le cache 6
6.4. Vider le cache 8

7. Utiliser le service Winsock Proxy 10
7.1. FTP et le mode FTP Passif 10
7.2. Vérifier la connexion entre le client WSP et le serveur Proxy 12
7.3. Mettre à jour les informations et la configuration du client 13
7.4. CREDTOOL 14
7.5. Notions avancées 15

8. Mettre en place de la sécurité d'accès 18
8.1. Internet Explorer prompte l'utilisateur anormalement 18
8.2. Définir des permissions pour un ou plusieurs protocoles 18
8.3. Spécifier un compte à la connexion 22
8.4. Le serveur Proxy et les permissions des serveurs Web 22

9. Déployer les clients 23
9.1. Déployer l'installation 23
9.2. Déployer la configuration 23

10. Mettre en place plusieurs serveurs Proxy si nécessaire 27
10.1. Le script de configuration automatique 27
10.2. Les chaînes de Proxy 27
10.3. Les tableaux de Proxy 30
a) La mise en place 30
b) Le protocole CARP 32
c) La tolérance de pannes 34

11. Intégrer Proxy avec des services et des serveurs existants 35
11.1. Le "Web Publishing" 35
11.2. Mettre en place une DMZ 36
11.3. Le "Reverse Proxying" 6
a) Considérations générales 6
b) Un exemple détaillé et classique: Exchange 6

12. Administrer son serveur 9
12.1. Le Microsoft® Proxy Server Web Administration Tool 9
12.2. Arrêter et redémarrer les services 9
12.3. Les logs Proxy sur ODBC 9
12.4. Les compteurs de performance 9
12.5. Utilisation des alertes 10
12.6. Le futur: Hit List Proxy Analyzer (HLPA) 11

13. Conclusion 12

Introduction

Pour une personne ne connaissant pas le produit Microsoft Proxy serveur 2.0, la prise en main s'effectue en général de la manière suivante:

0. information sur les fonctionnalités de base (Service Web Proxy, Service Winsock Proxy, Service Socks Proxy, la LAT, la sécurité, le filtrage de paquet...)
1. installation d'un serveur
2. la connexion entre le serveur Proxy et le réseau interne
3. la connexion entre le serveur Proxy et le réseau externe
4. protéger le réseau local de l'extérieur
5. installation d'un client
6. utiliser le service Web Proxy
7. utiliser le service Winsock Proxy
8. mettre en place de la sécurité d'accès
9. déployer les clients
10. mettre en place plusieurs serveurs Proxy si nécessaire
11. intégrer Proxy avec des services et des serveurs existants
12. administrer son serveur

Ce document ne traitera pas du premier point et assume que les connaissances de bases requises pour la mise en place et le support de Proxy serveur en général sont acquises.

Ce document a pour but, pour tous les autres points, de donner des informations supplémentaires et d'exposer des configurations avancées.

1. Installation d'un serveur

1.1. Rôle du serveur

Il est préférable d'installer Proxy Serveur sur un serveur autonome, ainsi le serveur gère sa propre base d'utilisateurs indépendamment de celle du réseau NT. Mais dans le cas où le réseau est important avec plusieurs serveurs Proxy il est également envisageable d'installer les serveurs dans un domaine à part et d'installer le premier serveur Proxy sur un PDC. Une fois ce domaine établi, il faut alors mettre en place une relation d'approbation unidirectionnelle: le domaine du ou des serveurs Proxy approuvant le domaine de travail. Ainsi les contrôle d'accès pourront être mis en place directement en se basant sur les comptes du domaine NT privé.

1.2. Installation par ligne de commande

Il est possible d'installer Proxy serveur par ligne de commande:

setup [***/r***] [***/u***] [***/k***] ***"****keynumber****"***

où:

/r réinstalle Proxy Serveur.

/u désinstalle Proxy Serveur mais laisse les composants partagés.

/k "*clé****"*** pour renseigner la clé du CD. Ce numéro doit être entre guillemets et sans aucun tiret ou espace (sinon le setup s'arrête sans aucunes explications)

1.3. Installation en Unattended

Une installation automatique permet d'installer Proxy serveur sans aucune interaction de la part de l'utilisateur.
La commande est la suivante:
stpwrapp [***/sms***] ***/k "****keynumber****"***
où:

/sms qui est requis si vous n'utilisez pas STPWRAPP avec SMS (Systems Management Server).

/k "*clé****"*** pour renseigner la clé du CD. Ce numéro doit être entre guillemets et sans aucun tiret ou espace (sinon le setup s'arrête sans aucunes explications)

La désinstallation peut également s'effectuer à partir d'une ligne de commande:
setup /qt /u.

Les réponses aux questions habituellement posées par l'interface d'installation doivent être renseignées dans un fichier Proxy.ini. Si une réponse n'est pas fournie dans ce fichier, le programme d'installation utilisera une valeur par défaut.

Le tableau suivant décrit les entrées et les valeurs qui sont possibles de spécifier dans un fichier Proxy.ini:

Section	*Entry*	Description
[Install]	Install Dir	Specifies the installation directory for Microsoft Proxy Server. If

		not specified, defaults to the first disk drive with enough space. Syntax is *drive:\directory*.
[Install]	Override Existing Config	If set to 0, Setup program retains existing configuration set by previous installation, ignoring data from the remaining sections of this file. Default is 0.
[Install]	Keep Array Membership If Exist	Applies to a Proxy Server computer that is configured as part of an array. If set to 1, Setup program retains the existing configuration rather than setting a default configuration. Default is 1.
[Client Access Config]	Set WinSock Proxy Access By IP Rather Than By Name	If set to 1, Setup writes the IP address into the [Server IP Addresses] section in the Mspclnt.ini file. If set to 0, Setup writes the computer name into that section. Default is 0.
[Client Access Config]	WinSock Proxy Access Control Enabled	If set to 1, access control for the WinSock Proxy service is enabled. Default is 1.
[Client Access Config]	Web Proxy Access Control Enabled	If set to 1, access control for the Web Proxy service is enabled. Default is 1.
[Client Access Config]	Computer Name	Specifies the computer or DNS name of the server.
[Client Access Config]	Set Browsers To Use Proxy	If set to 1, client Setup program configures the client computer's browser to use the proxy server defined in the WWW Proxy field. If set to 0, prevents the client Setup program from configuring clients to use a proxy server. This field has no effect on the client Mspclnt.ini file.
[Client Access Config]	WWW-Proxy	If ***Set Browsers To Use Proxy*** is set to 1, the client Setup program configures client browsers to use the proxy server named here. This field has no effect on the client Mspclnt.ini file.
[Client Access Config]	WebProxyPort	If ***Set Browsers To Use Proxy*** is set to 1, the client Setup program configures client browsers to use the port specified in that field. This should be the same port number that is set for the WWW service of Internet Information Server.
[Cache Config]	Drive	Specifies the disk drive to be used for caching. If not specified, defaults to the first NTFS partition large enough for adequate caching. The drive specified must have at least one NTFS partition, otherwise Setup fails.
[Cache Config]	Size	Specifies the minimum and maximum sizes (in megabytes) to be reserved on the drive specified in the Drive field for caching. The default values are 100 100.
[LAT Config]	Include Private Ranges	If set to 1, includes internal IP address ranges in the LAT. Syntax is ***10****.x.x.x*. At least one entry in this section is required; otherwise Setup fails.
[LAT Config]	Include	If set to 1, treats all network adapter IP address ranges as

	Ranges From All Cards	being on the internal network. Assumes a dial-up modem connection to the Internet. At least one entry in this section is required, otherwise Setup fails.
[LAT Config]	Range1,Range2...	Defines LAT IP ranges specifically. Syntax is ***Range1=****x.x.x.x*. ***Range2=****y.y.y.y*. At least one entry in this section is required, otherwise Setup fails.

Remarque: Comme le fichier Proxy.ini est présent sur le CD, vous ne pourrez modifier le fichier d'origine. Il est recommandé de copier le fichier en question à la racine du disque dur sur l'ordinateur ou sera lancée l'installation de Proxy Serveur. L'installation automatique cherche d'abord Proxy.ini à la racine du premier disque dur de la machine puis, s'il n'est pas trouvé, lit celui se situant sur le CD.

1.4. Ne pas oublier le fichier journal d'installation !

Le programme d'installation crée un fichier journal, C:\Mpssetup.log. Ce dernier est écrasé à chaque installation du produit. Il reste le premier endroit où analyser les causes d'un éventuel échec d'une installation.

1.5. Mettre en place le SP1

Le service pack 1 de Proxy a été mis à disposition sur le Web le 24 août 99. Il est téléchargeable depuis http://www.microsoft.com/proxy/Support/proxyupdate.asp
Il rassemble les correctifs inclus dans le "Proxy combined hotfix", plusieurs hotfixs postérieurs à ce dernier et deux ajouts de fonctionnalité:

- **Gestion des exceptions de routage:** Permettant d'indiquer à un serveur configuré pour router ses requêtes Web Proxy à un serveur upstream de ne pas router la totalité de ses requêtes et de gérer quelques exceptions de domaines a traiter localement (Q228271)
- **Une option pour enregistrer les années dans le fichier journal avec 4 chiffres.**

Le SP1 ne s'installe que sur des machines NT4 SP4 et s'accompagne d'une possibilité de désinstallation.

Voici une liste des articles rassemblant les correctifs inclus dans le SP1:

Article ID	Title
Q176922	Multiple IP Addresses Cause Dynamic Packet Filter to Fail
Q176958	Socks Port Number Always Shows as Zero (0) in Permission List
Q177154	Access Control Causes Reverse Proxy to Fail
Q177906	Caching Does Not Work Under Reverse Proxying
Q183282	IE via Proxy to IIS May Stop on Page with scripts
Q183749	Access Violation in INETINFO:TerminateExtension
Q183755	More Than One Internal IP with Socks Enabled Causes Dr. Watson
Q191414	Delayed Response to HTTPS Requests w/ Proxy 2.0 over IIS 4.0
Q222948	Cannot Download Large Files Using Proxy Server Combined Hotfix
Q225342	Err Msg: The Specified Method Is Not Supported
Q228540	Proxy Server Fix: Msplog.dll Changed to Record 4 Digit Year

Q228271	Proxy Server Forwards Requests When Part of a Web Proxy Chain
Q228837	Access Violation When Using Aventail Connect with SOCKS Proxy
Q231050	Proxy Server 2.0 Log Records May Contain Unsafe Characters
Q238572	FTP request through web proxy fails if file has no extension
Q238580	Active cache stops working after 10 name resolution failures
Q238803	Web Proxy Causes AV Allocating Large Block on Computer 1GB RAM
Q238808	Socks Doesn't Log Connection Until Connection Is Closed
Q239086	Proxy Can't Detect Local IP Range If Windows NT SP4 Is Installed
Q239495	Proxy User May Receive Old Data from a Web Site

1.6. Proxy 2.0 et Windows 2000

Proxy 2.0 fonctionne sur Windows 2000, il faut alors considérer deux cas selon que Proxy doit être installé sur une machine Windows 2000 neuve ou selon que le logiciel Proxy se trouve sur une plate-forme NT4 à mettre à jour vers Windows 2000.
Dans les deux cas, il est nécessaire de disposer de l'assistant de mise à jour téléchargeable depuis http://www.microsoft.com/proxy/Support/win2kbeta3.asp

- Installer Windows 2000 sur une plate-forme neuve: lancer l'assistant, l'interface demandera d'insérer le CD de Proxy 2.0.
- Mettre à jour un serveur Proxy sur NT4 existant vers Windows 2000: la procédure impose de faire une sauvegarde Proxy de la configuration de Proxy Serveur, de désinstaller Proxy Serveur, de mettre à jour Windows, d'installer Proxy Serveur (voir point précédent) puis de faire une restauration de la configuration Proxy.

L'installation par l'assistant de mise à jour inclus le SP1, il ne faudra pas installer le SP1 par la suite sur le poste Windows 2000.

2. La connexion entre le serveur Proxy et le réseau interne

2.1. Le nombre de cartes réseau

Bien que la configuration standard consiste à avoir deux cartes réseau sur une machine Proxy Serveur, une connectée au réseau interne et l'autre connectée au réseau externe, il est possible d'installer Proxy sur une machine ne disposant que d'une carte. Cette configuration s'applique en général dans le cas d'une mise en place d'un serveur agissant uniquement en tant que cache Web Proxy ou d'une chaîne de Proxy.
Dans ce cas il est à noter que:

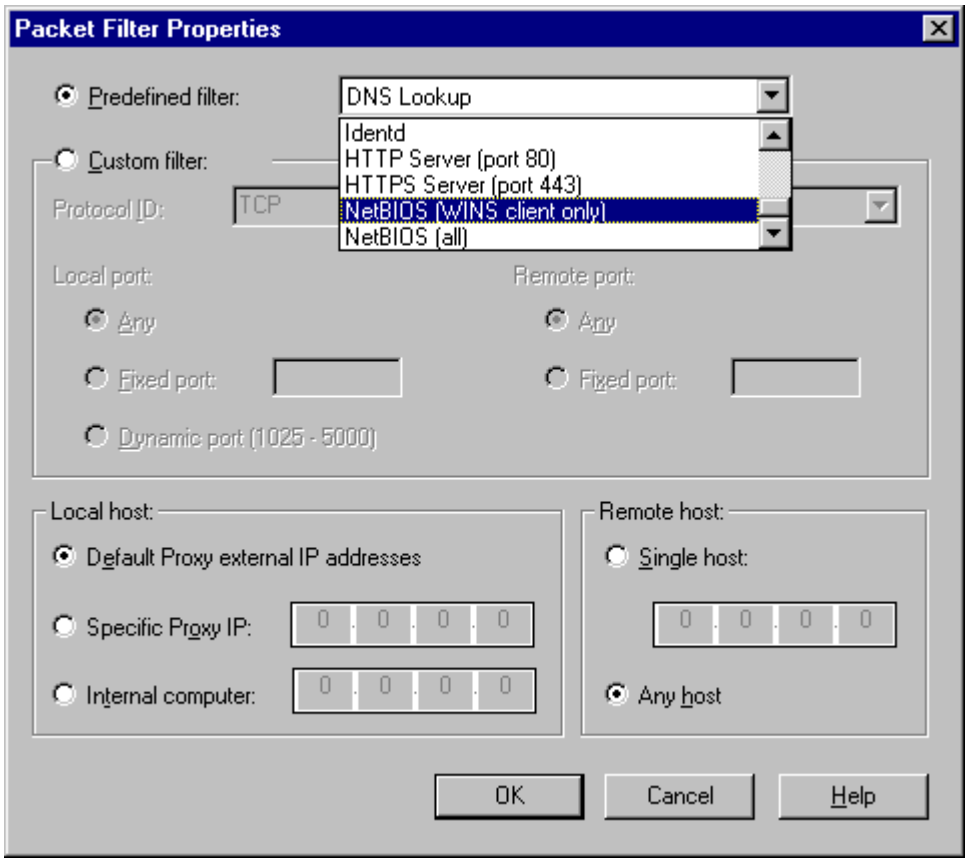
- il est impossible d'activer du filtrage de paquet.
- le service Winsock Proxy n'est pas fonctionnel et Microsoft conseille fortement de le désactiver.

2.2. Le protocole Netbios

La carte externe est normalement connectée à un réseau étranger tel que l'Internet (via un ISP ou pas). Il est toutefois possible que la carte externe soit reliée à un réseau privé (dans le cas d'une chaîne de Proxy par exemple) et que les autres services NT installés sur la machine aient besoin du protocole Netbios sur cette interface (exemples: le service "explorateur d'ordinateur", le service NetLogon, les services Exchange, etc...).
Dans le cas contraire il convient de désactiver le client WINS dans les liaisons de la carte réseau externe du serveur.
Dans les deux cas, il faut prendre garde à l'activation du filtrage de paquet.

Remarque: En cas de résolution d'un problème quelconque avec Proxy Serveur, il est judicieux dans un premier temps de retirer tout filtrage de paquet, de domaine et toute permission pour déterminer si le problème a sa source dans l'installation, la connexion, la configuration ... ou si c'est la mise en place de la sécurité qui en est la cause.

Par défaut, activer le filtrage de paquet sur la carte externe va rendre impossible toute communication NetBios. Par le biais des filtres on pourra soit rendre possible l'écoute du protocole Netbios sur la carte, soit considérer tout protocole NetBios reçu sur cette carte comme une agression éventuelle ou pas. Vous avez donc le choix entre deux filtres:



- **Le filtre prédéfini "NetBIOS (client WINS seulement):** C'est le filtre à employer quand le client Wins est activé sur la carte externe (i.e. on a besoin du protocole NetBios). Le protocole Netbios est donc écouté sur la carte mais il est garanti qu'aucun paquet NetBios ne va transiter du réseau externe vers le réseau interne (sauf si le routage IP est activé, nous verrons cela plus tard)
- **Le filtre prédéfini "NetBIOS (tous):** C'est le filtre à employer quand le client Wins est désactivé sur la carte externe (i.e. on n'en a pas besoin) mais que la réception de paquets utilisant le protocole NetBios est considérée comme normale par le serveur. Si ce Filtre n'est pas activé, tout trafic NetBios sera considéré comme une agression éventuelle et donc entraînera une écriture dans le journal et une génération de courrier électronique (si mis en place).

3. La connexion entre le serveur Proxy et le réseau externe

3.1. Utilisation d'une carte réseau pour se connecter au réseau externe

C'est le cas général, il convient alors s'assurer des points suivants:

- Le routage IP ne doit pas être activé.
- Les adresses des deux cartes doivent se trouver dans des sous-réseaux IP différents.
- Le paramétrage IP doit disposer d'une passerelle par défaut dont l'adresse IP fait partie du sous-réseau IP de la carte externe.
- Les adresses des serveurs DNS, qui sont en général ceux de l'ISP, ne doivent pas faire partie en conséquence du sous-réseau IP interne. Elles doivent donc être soit dans le réseau externe soit dans un réseau étranger et donc joignables uniquement via la passerelle par défaut.

3.2. Utilisation d'un modem

Dans le cas ou l'interface de connexion au réseau externe est un modem, les problèmes classiques concernent soit un mauvais paramétrage du modem soit le paramétrage de l'auto-déconnexion du modem lorsque aucune activité n'est détectée sur la ligne.

L'autodial de Proxy serveur s'appuie sur les fonctionnalités de numérotation de NT serveur. Les précautions à prendre sont donc liées à l'utilisation conflictuelle qui pourrait être faite du modem entre le service RAS et Proxy.
Il convient de s'assurer que:

- Le service "Gestionnaire de numérotation automatique d'accès" est désactivé
- Le service "Gestionnaire de connexion d'accès distant" est activé
- Aucun appel ne peut arriver sur le modem (en clair, dans le paramétrage du service RAS, configurez l'interface modem utilisée par le Proxy pour n'autoriser que les appels SORTANTS)
- Les paramétrages de Proxy ne rentrent pas en conflit avec ceux du carnet d'adresse RAS

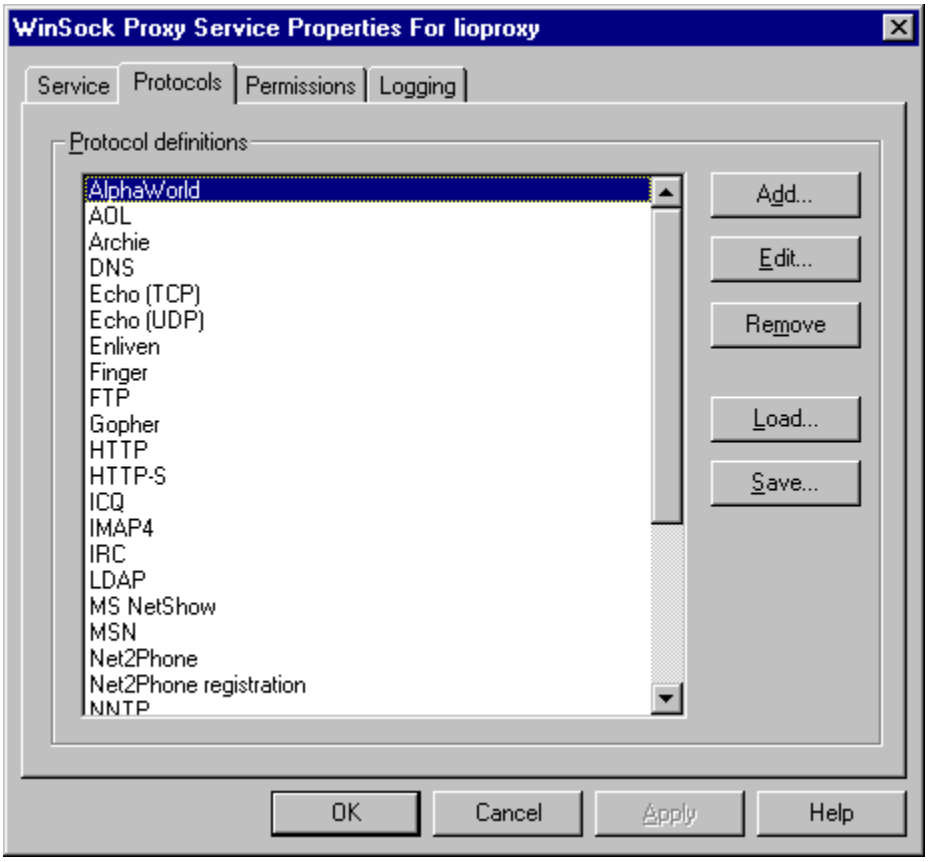
Ces informations sont détaillées dans les articles techniques Q181407, Q222053 et Q17254 (fiche Française).

4. Protéger le réseau local de l'extérieur

4.1. Rappels sur les différentes définitions dans l'interface

Il est commun de mélanger les deux interfaces permettant de définir les protocoles à employer avec le service Winsock Proxy et le filtrage de paquet.

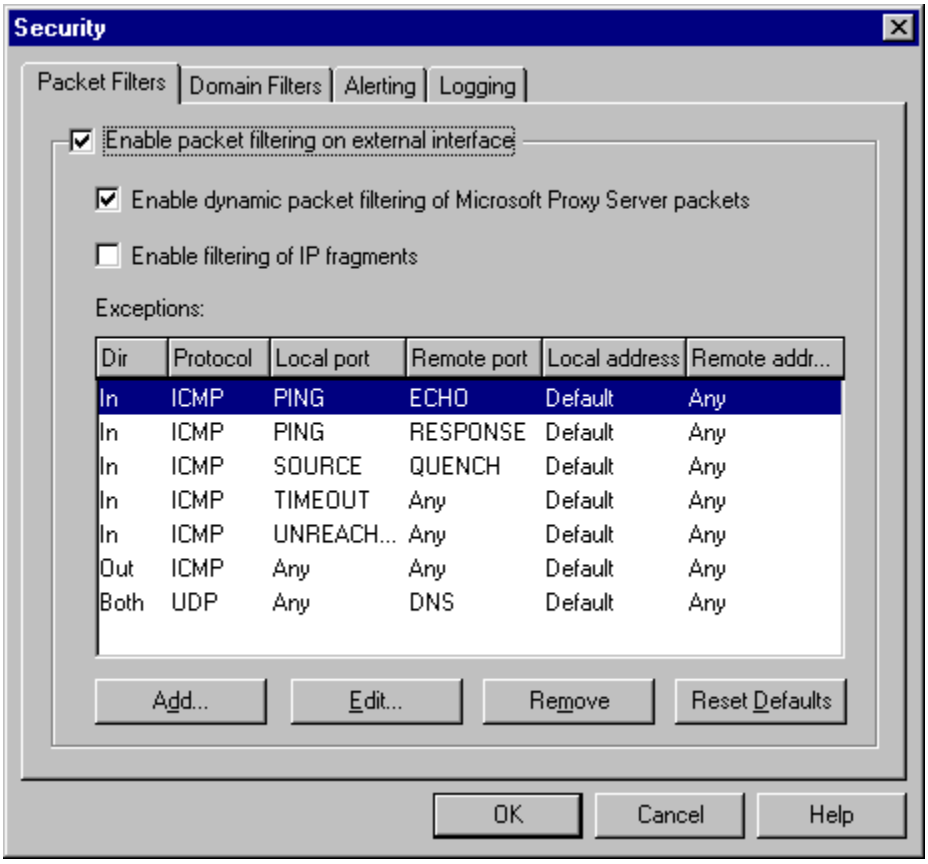
- **L'onglet "Protocoles" des propriétés du Winsock Proxy Service:** C'est là que vont être définis les protocoles liés aux APPLICATIONS WINSOCKS. En fait, y sont définit les ports sur lesquels vont se faire les appels Winsock. Ainsi il est normal de retrouver HTTP car IE est une application qui fait des appels Winsock sur le port 80. Du coup il est envisageable d'utiliser un Internet Explorer sur un poste client, de ne pas le configurer pour attaquer un WEB Proxy, d'y entrer une URL du type www.mondomaine.com (pour s'assurer que la requête ne soit pas résolue localement) et quand il va falloir résoudre cette demande d'abord la résolution du nom va passer par GetHostByAddr (Winsock DNS sur port 53) et ensuite l'application IE va faire des requêtes Winsock sur le port 80... donc cela passe par le service Winsock proxy !



Dans l'onglet Permissions des propriétés du Winsock Proxy Service on va définir des "access control" sur ces fameuses "applications" Winsock définies dans l'onglet précédent.

- **L'onglet "Packet Filters" accessible via le bouton "Security" dans les propriétés de n'importe quel service Proxy:** C'est là que vont être définis les

filtres à appliquer sur la carte externe (voir point suivant). Ils n'ont aucun point commun avec les protocoles Winsock. Le seul lien qui relie ces deux points est résumé dans cette phrase: il faut s'assurer que les filtres permettent de laisser passer, entre autre, les protocoles Winsocks à utiliser. Cette condition est remplie dés que la case à cocher de filtrage de paquet dynamique est cochée.



4.2. Le filtrage de paquets

Proxy Serveur agit également en tant que pare-feu, c'est la fonctionnalité de filtrage de paquets qui n'est possible que si deux cartes réseau sont présentes.

- Ce filtrage se fait sur la carte externe.
- Il est indépendant du fait que le routage IP soit activé ou non.
- Il est de plus non configurable par utilisateur (on ne peut définir des filtres spécifiques pour tel ou tel groupe d'utilisateur ou utilisateur)
- Dés que l'option est activée, tous les paquets sont jetés à l'exception de ceux indiqués dans la liste "exceptions".

Dés que le filtrage est activé, si la case "Enable dynamic packet filtering of Microsoft Proxy server packets" est laissée cochée (par défaut) , les paquets correspondants aux services Proxy peuvent toujours passer. C'est à dire:

- les protocoles Winsock définis dans les propriétés du "Winsock Proxy service et ceci dans le sens Intranet vers Internet uniquement (tout ce qui vient de l'extérieur ou émis directement par le serveur Proxy lui-même vers l'Internet).
- les protocoles Web Proxy: HTTP, HTTPS, GOPHER et FTP READ

- les protocoles SOCKS

Il est conseillé de garder cette option cochée car si elle ne l'est pas, certes le filtrage du serveur sera plus pointu mais il faudra bien définir tous les filtres correspondant à ce qu'il est possible de laisser passer. En clair il faudra s'assurer que pour tout protocole Winsock définit et qui ne doit pas être filtré, qu'un filtre puisse laisser passer tout trafic relatif a ce protocole (équivalent à une double saisie).

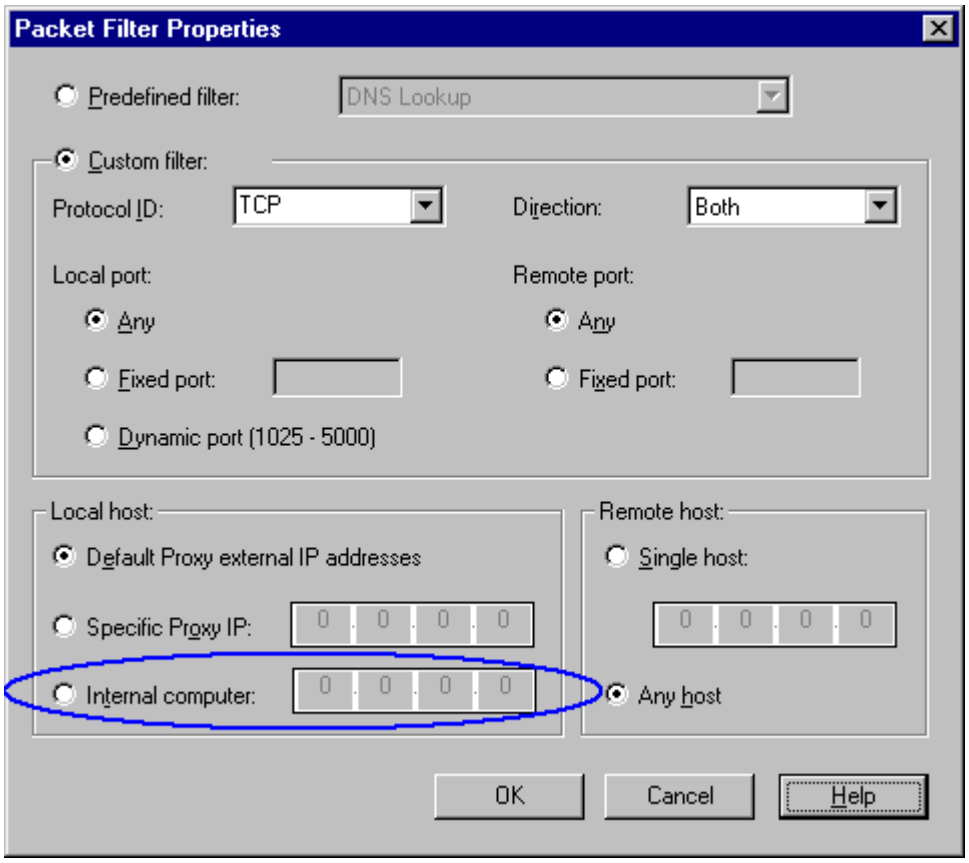
4.3. Le filtrage de paquets et les protocoles non gérés par les services Proxy

A leur création, les filtres sont par défaut basés sur une émission depuis la carte externe du serveur Proxy. En effet, en général, tout trafic qui passe à travers le serveur Proxy est pris en charge par un service Proxy.

Si ce n'est pas le cas, une autre adresse doit être spécifiée comme adresse à l'origine du paquet dans la création de filtres, cela signifie que le protocole n'est pas géré par un service Proxy et dans ce cas, il faut que cette adresse ne soit pas dans la LAT.
Toute tentative de création d'un filtre avec une adresse IP autre que l'adresse externe du serveur Proxy se solde par un message d'erreur à la validation de l'interface " An Invalid Local Host Address was specified for a packet filter".

Expliquons cette remarque par l'exemple: Supposons qu'un administrateur veuille qu'un poste de son intranet puisse pinger un serveur du côté externe de son Proxy. Sachant que la commande PING n'est ni un protocole géré par le service Web Proxy, ni un applicatif Winsocks ou Socks, il faut non seulement que le ping puisse transiter de l'intranet vers l'extérieur (routage IP) mais en plus il faut ajouter un filtre sur ICMP en spécifiant l'adresse de l'ordinateur à l'origine du paquet. Or toute création d'un filtre spécifiant une telle adresse impose que la dite adresse ne soit pas dans la LAT (Q176376), le poste doit donc être dans une DMZ par exemple (voir chapitre 11).

En conclusion: pour tout protocole non géré par les services Proxy (HTTP, HTTPS, GOPHER, FTP READ, Winsock ou Socks), il faut que routage IP soit activé et que l'adresse à l'origine du trafic ne soit pas dans la LAT.



4.4. La checklist

Comme un serveur Proxy est la porte de sortie de votre réseau vers l'Internet il en constitue également la porte d'entrée depuis l'extérieur. La liste suivante est une sorte de checklist résumant les principaux points à garder à l'esprit en mettant en place un serveur Proxy:

- Les considérations standards sont toujours valables: stratégie de mot de passe forte, bien gérer ses groupes d'utilisateurs et les appartenances aux groupes fondés de pouvoir (administrateurs, opérateurs de serveur), gestion des partages réseau et de leur accès, droits NTFS, etc...
- Désactivez le routage IP.
- Activez le contrôle d'accès (voir le chapitre 8).
- Ne jamais ajouter d'adresses IP externes dans la Table d'adresses locales
- Activez le moins de liaisons possibles entre des services et protocoles NT et la carte externe (protocole Netbios, protocole IPX, service Serveur, service Workstation, ...)
- Assurez-vous que vos clients passent par votre Proxy en supprimant toute configuration DNS ou passerelle par défaut
- Désactivez les ports écoutant les appels RPC sur la carte externe (1024 à 1029): Pour cela, notez l'identification de votre carte interne sous HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services, ensuite créez une nouvelle arborescence de clés sous la clé Services: RPC\Linkage\Bind. Dans la clé Bind, créez une nouvelle valeur de type chaîne dont le contenu est l'identification de votre carte interne.

5. Installation d'un client

5.1. Utilisation du service Web Proxy

Pour utiliser ce service, il suffit de disposer d'un browser dit "CERN PROXY compliant" tel qu'Internet Explorer et le configurer pour utiliser un Proxy.

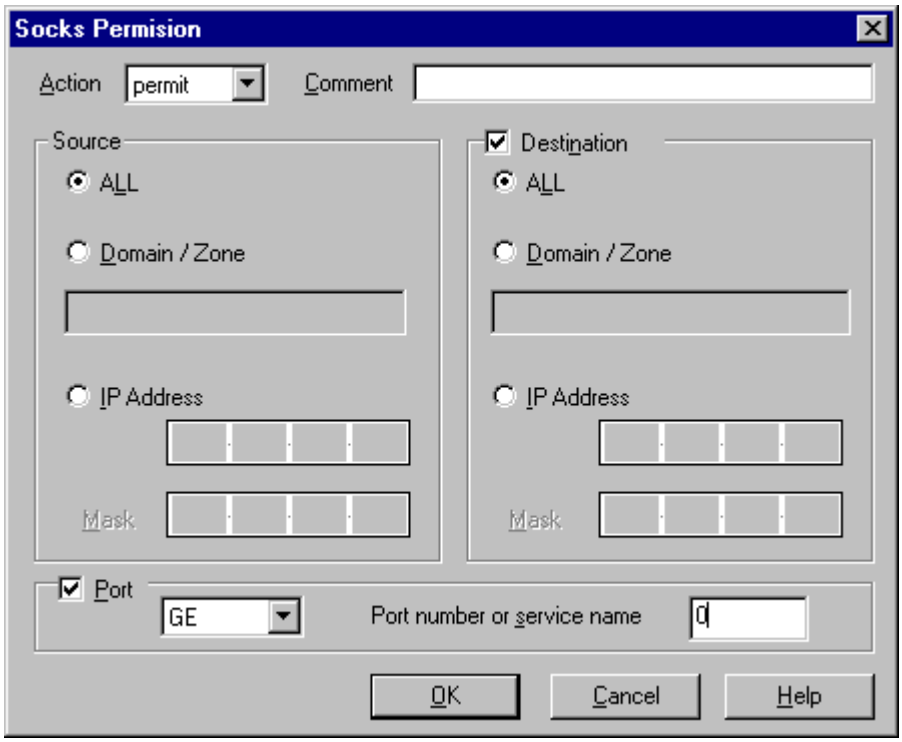
5.2. Utilisation du service Socks Proxy

Pour utiliser le service Socks proxy il faut disposer sur la machine cliente d'un applicatif client Socks ET qui est configurable pour utiliser un serveur Proxy
Pour utiliser le service Socks, les éléments suivants sont à prendre en compte:

- Le service SOCKS Proxy de Ms-Proxy 2.0 ne supporte que la version 4.3a de SOCKS. Si un applicatif est basé sur une autre version de SOCKS, il est incompatible avec Ms-Proxy 2.0
- Le service SOCKS Proxy de Ms-Proxy 2.0 ne supporte pas les applications clientes basées sur le port UDP comme RealAudio, VDOLIVE, NetShow
- Le service SOCKS Proxy de Ms-Proxy 2.0 ne supporte pas le protocole IPX/SPX.
- Le service SOCKS Proxy ne s'appuie pas sur un client Proxy comme Winsock
- Par défaut, toutes les requêtes SOCKS sont rejetées par PROXY. On doit, en premier test, rajouter une entrée dans l'onglet "Permissions" du service SOCKS pour tout laisser passer:

  Action: Permit
  Source: All
  Destination: All
  Port: GE 0

  ... puis restreindre ce filtre si nécessaire.



- Il est conseillé de désactiver un éventuel client Winsock installé sur le poste du client SOCKS.
- Avec certains serveurs l'utilisation de Identd est nécessaire:
"
The Identd Simulation Service:
In addition to being used by the Socks Proxy service, some Internet servers also require users to identify themselves before allowing access to certain services. For example, an IRC service or an FTP service might require a unique identifier for each user. The Identd Simulation service, Identd.exe, provided on the Proxy Server compact disc supplies a random, false user name to those servers that would otherwise block Microsoft Proxy clients from gaining access to services.

Identd.exe must be installed manually. After this service is installed, it appears in Control Panel under Services and starts automatically after the server computer is restarted.
"
- Il n'est pas possible de chaîner des serveurs SOCKS

5.3. Installation du client Winsock Proxy en ligne de commande

Il est possible d'installer le client Winsock Proxy par ligne de commande :

setup [***/r***] [***/u***] [***/q***[***1***, ***t***]]

où:

/r réinstalle le client

/u désinstalle le client mais laisse les composants partagés

/q pour une installation silencieuse

/q1 est une installation silencieuse comme ***/q*** sans même la boite de dialogue pour confirmation de l'installation

/qt est une installation silencieuse comme ***/q1*** sans même la barre de progression

5.4. Installation en Unattended

Une installation automatique permet d'installer le client Winsock Proxy sans aucune interaction de la part de l'utilisateur.
Elle se base sur les données renseignées dans le fichier Proxy.ini qui se trouve sur le partage Mspclnt du serveur. Ce fichier n'a qu'une seule entrée, elle spécifie le répertoire où installer le logiciel:

```
[Proxy Setup Install]
Install Dir=C:\Mspclnt
```

Remarque: Comme le fichier Proxy.ini est présent sur le CD, vous ne pourrez modifier le fichier d'origine. Il est recommandé d'utiliser le fichier sur le partage mspclnt.

5.5. Ne pas oublier le fichier journal d'installation !

Le programme d'installation crée un fichier journal, C:\Mpcsetup.log. Ce dernier est écrasé à chaque installation du produit. Il reste le premier endroit où analyser les causes d'un éventuel échec d'une installation.

5.6. Les fichiers du client Winsock Proxy

- **MSPCLNT.INI:** Fichier de configuration du client Winsock Proxy. Téléchargé par défaut et mis à jour sur le client à chaque redémarrage du client et toutes les six heures. Lorsqu'un Refresh a lieu, l'ordre des partages à utiliser qui est employé est celui listé dans la section [MASTER CONFIG] du fichier MSPCLNT.INI. Au minimum, une entrée doit être présente. Le chemin suivant est utilisé seulement si le précédent n'a pas permis de trouver le fichier de configuration
- **MSPLAT.TXT:** Quand un client Proxy est installé, ce fichier est copié dans le répertoire Mspclnt. C'est une copie de la LAT du serveur, le serveur la met à jour régulièrement.
  A chaque fois qu'une application Winsock essaie de faire une connexion avec une adresse IP, c'est cette LAT qui est utilisé pour savoir s'il faut passer par le Winsock Proxy Service ou pas.
  Quand on clique sur le bouton 'Update Now' du client Proxy, on relit la LAT et le fichier MSPCLNT.INI

Ces deux fichiers sont considérés comme les fichiers GLOBAUX de configuration.
A l'inverse du ou des fichier(s) spécifique(s) de configuration client :

- **LOCALLAT.TXT:** Fichier spécial pour le client de manière à avoir sa propre LAT. Ce fichier est a créer à la main et à placer dans le répertoire MSPCLNT. Il spécifie des adresses additionnelles à considérer comme internes.
- **WSPCFG.INI:** Fichier indiquant à l'application Intranet serveur pour faire un "remote listen". Il doit être mis dans le même répertoire que l'exécutable et n'a que la section suivante :

"

[<nom de l'application WSP CLIENT>]
ServerBindTcpPorts=400
KillOldSession=1
<et plein d'autres paramètres...que nous verrons plus tard>

"

Ci-après un exemple de fichier MspcInt.ini et un tableau de référence des paramètres qui peuvent le composer :

"

[wspsrv]
Disable=1
[inetinfo]
Disable=1
[services]
Disable=1
[spoolss]
Disable=1
[rpcss]
Disable=1
[kernel32]
Disable=1
[mapisp32]
Disable=0
[exchng32]
Disable=0
[outlook]
Disable=0
[raplayer]
RemoteBindUdpPorts=6970-7170
LocalBindTcpPorts=7070
[rvplayer]
RemoteBindUdpPorts=6970-7170
LocalBindTcpPorts=7070
[net2fone]
ServerBindTcpPorts=0
[icq]
RemoteBindUdpPorts=0
ServerBindTcpPorts=0,1025-5000
NameResolutionForLocalHost=P
[Master Config]
Path1=\\A-DANSIS2\Mspclnt\
[Servers IP Addresses]
Name=A-DANSIS2
[Servers IPX Addresses]
Addr1=55555555-000000000001
[Common]
Port=1745
Configuration Refresh Time (Hours)=6
Re-check Inaccessible Server Time (Minutes)=10
Refresh Give Up Time (Minutes)=15
Inaccessible Servers Give Up Time (Minutes)=2
Set Browsers To Use Proxy=1
WWW-Proxy=A-DANSIS2
WebProxyPort=80

"

Section	***Entry***	Description
[Master Config]	Path1	A UNC path to the shared network directory on the server, containing the master copy of the client configuration files. If participating in an array, the paths to the shared network directories of all array members. This section is required for backward compatibility with Microsoft Proxy Server version 1.0 clients.
[Servers IP addresses]	Name	The computer or DNS name (if there is a DNS server available) for the Proxy Server computer used by the client. If participating in an array, the DNS name for the array. (This entry does not appear if an IP address is used.)
[Servers IP addresses]	Addr1	The IP address of the Proxy Server computer used by the client. If participating in an array, the IP address of each array member. (This entry does not appear if a computer or DNS name is used.) Additional entries are shown as Addr2, Addr3, and so on. This entry can be used if there is not a DNS server available on your internal network.
[Servers IPX Addresses]	Addr1	The IPX address of the Proxy Server computer. If participating in an array, the IPX address of each array member. (This entry does not appear if a computer or DNS name is used.) Additional entries are shown as Addr2, Addr3, and so on. This entry can be used if there is not a DNS server available on your internal network.
[Common]	Port	The port Proxy Server uses for the control channel. This value is rarely changed. If it needs to be changed, edit the server's master copy of the Mspclnt.ini file. It should be changed only if there is a conflict with another service on the server. This value should never be edited in the client's copy of the Mspclnt.ini file.
[Common]	Configuration Refresh Time (Hours)	After this interval, specified in hours, the client asks the server to download a fresh copy of the Local Address Table (Msplat.txt).
[Common]	Re-check Inaccessible Server Time (Minutes)	For this interval, specified in minutes, the WinSock client does not try to redirect a request by using the specific inaccessible server. Default value is 10 minutes.
[Common]	Refresh Give Up Time (Minutes)	After this interval, specified in minutes, the WinSock client attempts to refresh the configuration if a previous refresh attempt has failed. Default value is 15 minutes.
[Common]	Inaccessible Servers Give Up Time (Minutes)	For this interval, specified in minutes, the WinSock client does not try to redirect a request if all servers are marked as inaccessible. After this interval, the client tries one of the servers even if the ***Refresh Give Up Time*** has not expired. Default value is 2 minutes.
[Common]	Set Browsers To Use Proxy	In the Proxy.ini file, set this value to 1 to have the client Setup program configure the client computer's browser to use the Proxy Server computer defined in the ***WWW Proxy*** field. Set the value to 0 to prevent the client Setup program from configuring clients to use a Proxy Server computer. This field has no effect on the client's version of the proxy.ini file.
[Common]	Configuration URL	The location of the configuration script that is downloaded to a client browser to use for routing into a particular Proxy Server computer in an array. The URL has the form ***http://****servername****/array.dll?Get.Routing.Script***, where *servername* is the name of the Proxy Server computer that stores the script.
[Common]	LocalDomains	A list of suffixes for names that are resolved locally, separated by commas. Domain names that end in the listed strings are resolved at the client.
[Common]	WWW-Proxy	In the Proxy.ini file, if ***Set Browsers to Use Proxy*** is set to 1, the client Setup program configures client browsers to use the Proxy Server

		computer named here. This field has no effect on the client's version of the file.
[Common]	WebProxyPort	The listen-on port used by the Web Proxy service. In the Proxy.ini file, if ***Set Browsers to Use Proxy*** is set to 1, the client Setup program configures client browsers to use the port named in that box. This should be the same port number that is set for the WWW service of Internet Information Server.

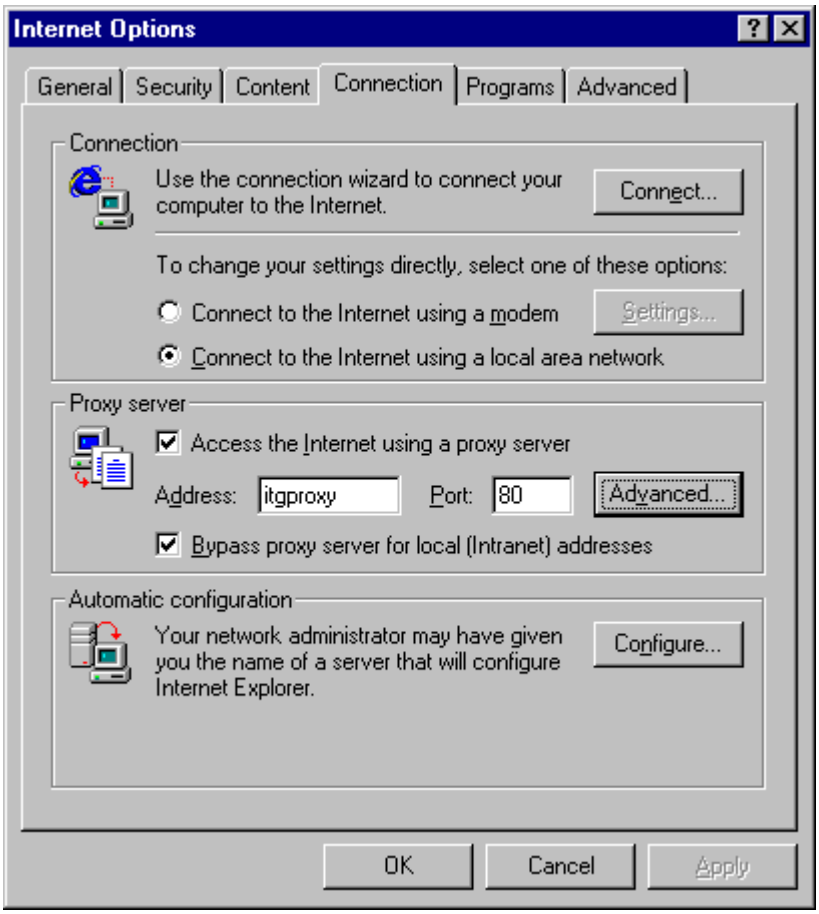
6. Utiliser le service Web Proxy

6.1. Configurer son browser

Pour utiliser les fonctionnalités du service Web Proxy, il faut configurer son browser et lui spécifier un "CERN COMPLIANT PROXY", c'est à dire un serveur Proxy auquel vont être transmises toutes les requêtes HTTP, HTTPS, FTP READ et GOPHER de l'utilisateur.

Les différents points sont à considérer en cas de problème d'utilisation de ce service Web Proxy :

- **La connexion ne se fait pas bien ou pas du tout :** Si le serveur Proxy a bien été spécifié, que ce dernier fonctionne localement (en utilisant un browser sur le serveur lui-même) et qu'il est possible d'accéder au serveur depuis le poste client (ping, net view...) la première chose à vérifier est qu'il n'y a pas de fichier de configuration automatique spécifié dans l'interface. Un tel fichier de configuration modifie le comportement de Internet Explorer avec des paramètres qui ne sont pas visibles dans l'interface mais qui ont préséance sur ces derniers.
  A titre de test, il est judicieux de ne pas spécifier de fichier d'autoconfiguration et vérifier si, dans ce cas, la connexion se déroule bien.

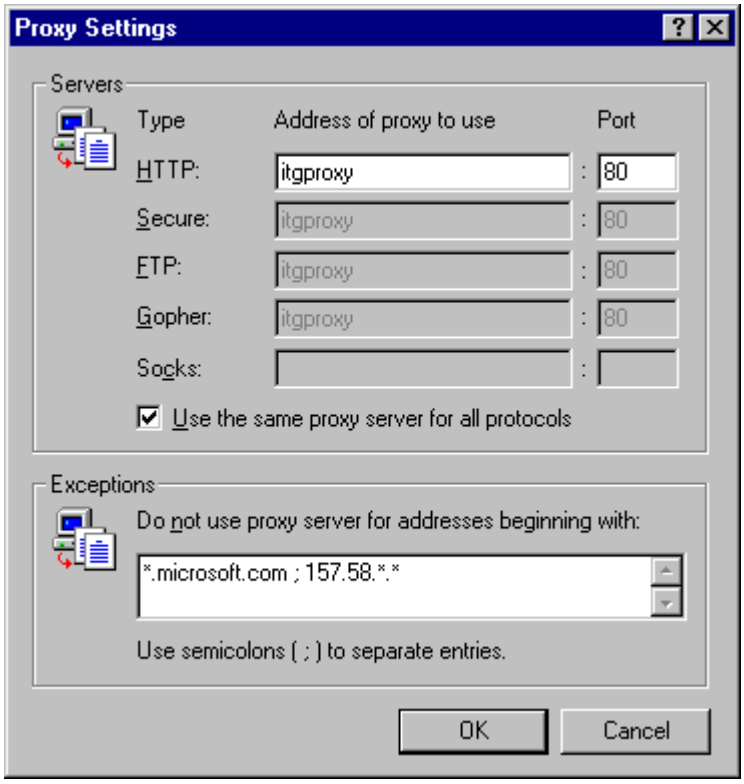


- **Le contournement du serveur Proxy :** La fameuse case à cocher "bypass proxy server for local (Intranet) Addresses" indique au browser de ne pas

contacter le serveur Proxy pour des requêtes locales. Comment sont définies ces adresses locales ? Tout simplement si l'URL a un point ou pas.
Le fait d'avoir un point dans l'URL fait que cette URL est déclarée comme devant être gérée par la "Zone Internet" dans IE. En conséquence :

- Le proxy peut donc être ignoré dans ce cas
- Les paramètres de sécurité de la "Zone Internet" vont donc pouvoir entraîner des comportements différents notamment en terme d'authentification. Par exemple si la zone Intranet est en niveau faible et si la zone Internet est en niveau haut, ce n'est pas à cause du Proxy que telle ou telle requête va demander une authentification ou pas - si on est en NTLM - mais parce que le browser va répondre au "challenge" de manière transparente ou va refuser de le faire et donc prompter l'utilisateur avant d'envoyer le "response"

En conclusion, il faut, pour tout serveur Intranet (a ne pas accéder avec un Proxy) soit le contacter avec un nom Netbios soit le spécifier dans les paramètres d'exclusion...



Attention: Les paramètres d'exclusion sont mal gérés avec IE4, il est possible que le fait d'avoir plusieurs exclusions en désactive d'autres. Donc dans le cas ou un problème apparaît sur un browser avec plusieurs exclusions il est judicieux de tester les exclusions une par une (entre chaque test, fermez et relancez IE)

6.2. Les critères de mise en cache

Dans la plupart une page n'est pas mise en cache si :
- elle ne contient pas de directives désactivant le caching au niveau du proxy (Cache-Control = Private)
- elle ne contient pas de directives désactivant le caching au niveau proxy et client (Pragma= no-cache , Cache-control: no-cache)
- c'est une page marquee comme expirant immédiatement (Expires:0)
- c'est une page ASP (par défaut: Cache-Control = Private)

"

Caching Criteria

A Web object must satisfy the following criteria in order to be cached:

• The request must be a GET.
• There must be no keywords, which are typically used for basic logons.
• The file must be served by the HTTP protocol (objects associated with other protocols are not cached).
• The HTTP response header must not include WWW-Authenticate , Pragma: no-cache, Cache-control: Private, Cache-control: no-cache, or Set-Cookie.
• The date in the Expires: header field must be later than the date in the Date: header field. The Expires: header is used in all HTTP requests to indicate a date and time for the request to expire on the network. The Date: header is used to indicate the date and time that the Web server received the request. Both fields are generically returned in almost all HTTP requests. Some Web servers indicate to downstream caches that a page should not be cached by setting the Expires: header equal to the Date: header, indicating that the page expires immediately. Also, setting this field to “Expires: 0” prevents caching as well.
• The HTTP Result code must be 200 (success).
• The object must not be encrypted or protected by Secure Sockets Layer (SSL).
• There cannot be an Authorization header in the HTTP request header, or Vary in the response header.

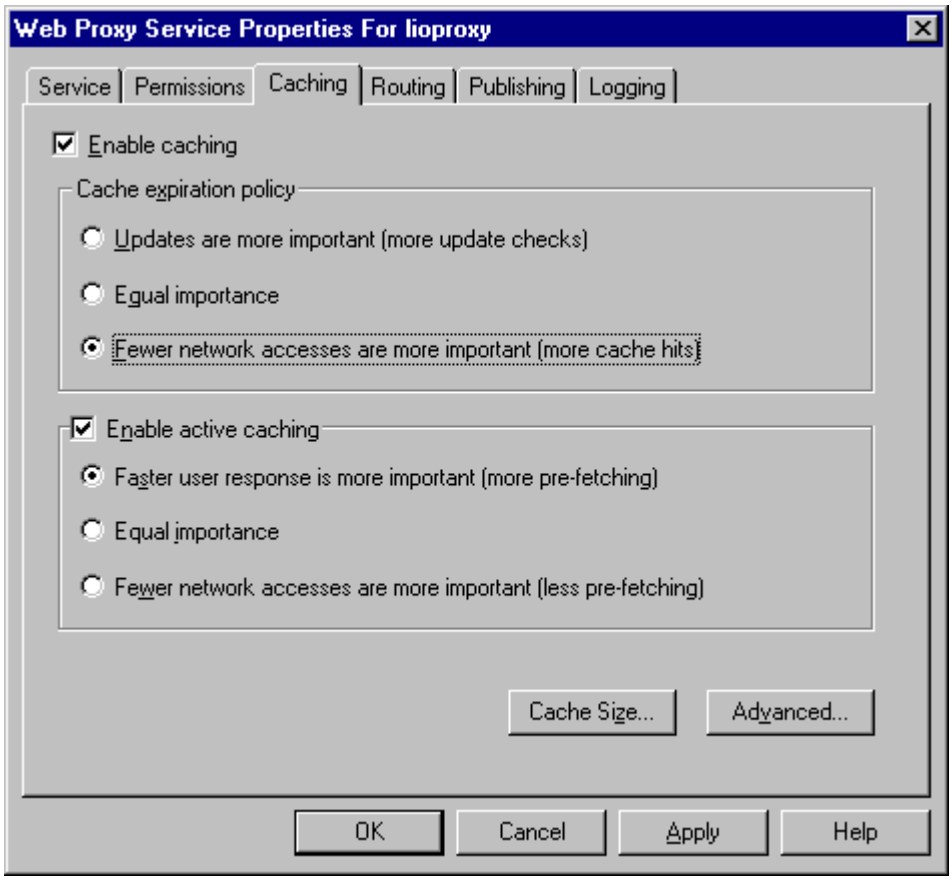
The HTTP header may include “cookies,” which allow a server to customize a response for a particular user. Cookies are increasingly used for custom pages or for informal (that is, not very secure) authentication. Microsoft Proxy Server treats cookies as another optional HTTP header that is disregarded, with the exception of the Set-Cookie header. It is assumed that subsequent transactions after the cookie has been set can be cached, unless any of the subsequent objects requested include headers with cache-ineligible exception values based on the criteria in the preceding list.
"

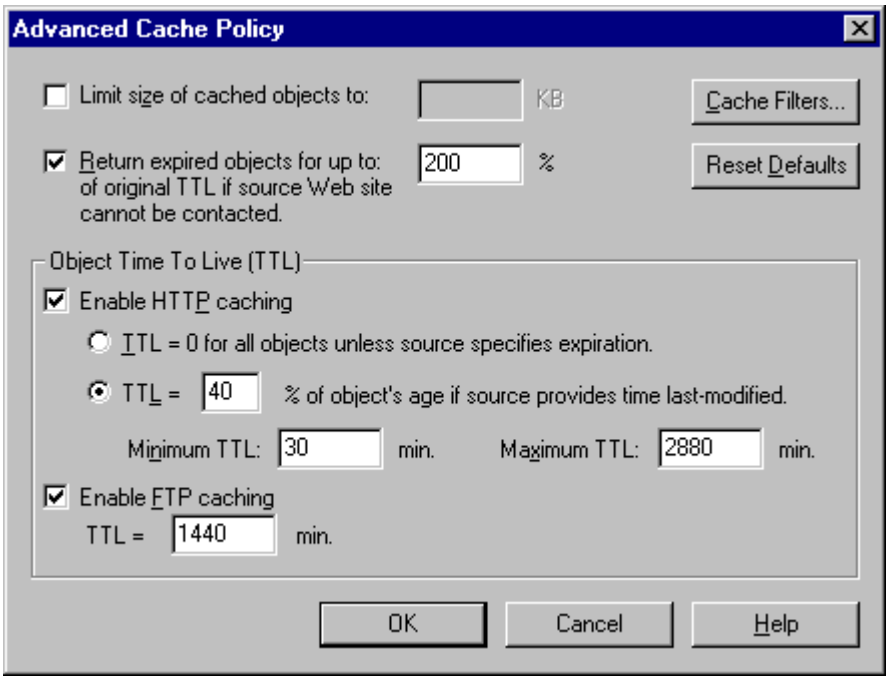
6.3. Favoriser le cache

Pour favoriser au maximum une utilisation du cache il convient de jouer sur les paramètres suivants:
- L'option "Fewer network accesses are more important (more cache hits) est à choisir.
- L'option "Active caching" diminue le nombre d'accès Internet dans le sens ou le serveur ira se mettre à jour tout seul pour des objets dont l'expiration approche

durant des périodes de faible activité du serveur. Ainsi, les futures requêtes sur ces objets seront satisfaites depuis le cache.

- Avoir une taille de cache conséquente
- Ne pas limiter la taille des objets cachés (par défaut)
- Augmenter la valeur "Return expired objects for up to X% of original TTL if source Web site cannot be contacted". Monter cette valeur jusqu'à 200 % peut être à la limite envisagée, il est rare d'utiliser une valeur supérieure...
- Jouer avec le TTL des objets HHTP cachés (pour une utilisation standard, il est conseillé de ne pas toucher à ces paramètres)



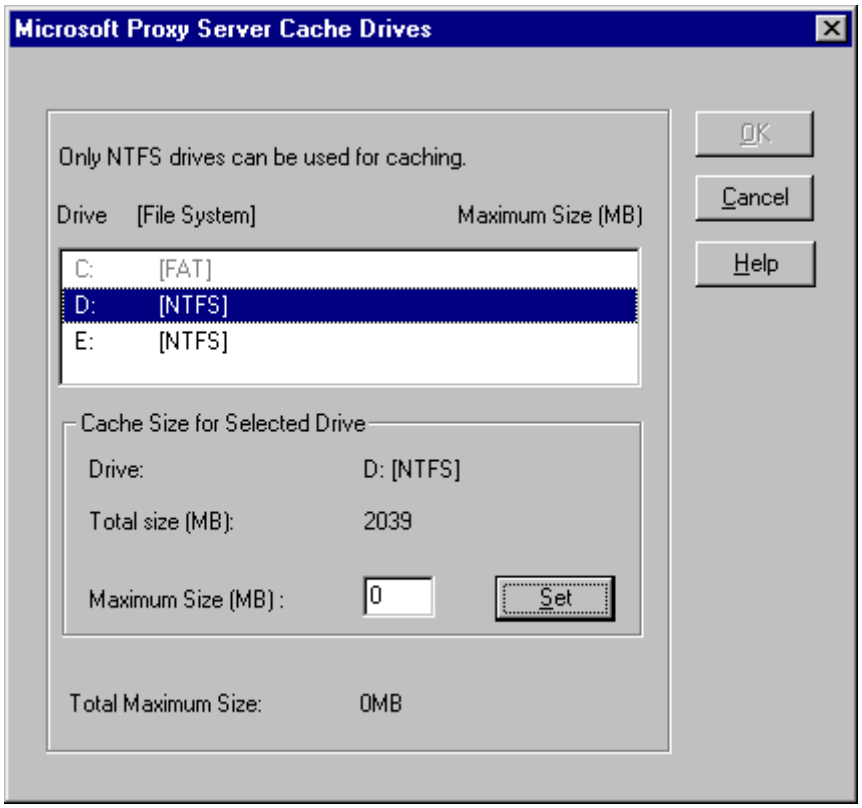


6.4. Vider le cache

Il n'y a pas d'interface pour purger le cache.

Les deux méthodes envisageables sont manuelles:

- Dans la configuration du cache Web Proxy configurez un nouveau cache sur le deuxième disque (taille minimum: 5 Mo) et détruisez le cache original. Arrêtez et redémarrez le service Web Proxy.
  Il vous reste alors a faire la manipulation inverse pour retrouver vos paramètres d'origine avec un cache vide.



- Arrêtez le service Web Proxy, effacez tous les sous répertoires du répertoire URLCACHE de votre disque dur. Redémarrez le service.

La gestion du nettoyage est liée à deux clés dans la base de registre:

CleanupInterval
DataType: REG_DWORD
Range: 0-93a40(h)
Default: 15180(h)
Description: The interval size in seconds between each cache cleanup. The default setting is for every 86,400 seconds (24 hours).

CleanupTime
DataType: REG_DWORD
Range: 0-23
Default: 0
Description: Sets the hour of the day that cache cleanup is scheduled to occur. The default is to set cleanup to occur at 12:00 A.M.

7. Utiliser le service Winsock Proxy

7.1. FTP et le mode FTP Passif

Nous avons vu que le service Web Proxy permet de gérer 4 définitions de protocoles:
- WWW
- Secure (https)
- Gopher
- FTP READ: c'est à dire seulement du FTP entrant dans le réseau intranet.

Conclusion: il n'est pas possible a travers ce service de faire du FTP "Sortant"

La seule solution à cette question consiste donc à employer un client FTP (Microsoft ou autre) basé sur Winsock en l'associant avec le client Winsock Proxy.

A ce moment là il faudra prendre en compte les points suivants:
- Si du filtrage de paquets est activé sur le serveur Proxy, alors il faut que les ports spécifiques à FTP soient autorisés à passer à travers le Proxy (voir fiche technique Q17478)
- Si la connexion avec le serveur FTP se fait en mode FTP passif et que le filtrage de paquets est activé alors il faut que ce mode de fonctionnement de FTP puisse passer à travers Proxy (sur Proxy2, cela est le cas par défaut, le protocole FTP étant défini avec une ligne "TCP inbound 0 for subsequent connections") (voir fiches Q163651 et Q177310)

Conclusion: Il faudra utiliser le FTP en ligne de commande, un utilitaire type CuteFTP OU encore IE5 qui présente une nouvelle fonctionnalité dite "FTP folders" (voir Q217888). Attention, si vous vous orientez dans cette solution IE5 prenez garde à la remarque en fin d'article:
"
If you are unable to see the FTP user interface, a CERN proxy server may be preventing you from doing so. You can verify this by connecting to the server using the Ftp.exe tool. To work around this issue, use a non-CERN proxy server such as Microsoft Remote Winsock.
"
En clair: La fonctionnalité FTP Folders ne fonctionne pas avec un CERN Proxy (dans notre cas le service Web Proxy) mais fonctionne bien avec un non-CERN Proxy (le service Winsock Proxy avec le client qui va avec). Donc vous NE DEVREZ PAS configurer votre IE5 pour utiliser un WEB Proxy ET configurer votre client Winsock pour utiliser le serveur Proxy.

Remarque: *le mode FTP Passif est à activer dés qu'un problème FTP est remonté en passant a travers Winsock. Le fait de l'activer ou non permet de savoir rapidement si le problème est lié à ce point et si cela vient du serveur Proxy ou du serveur FTP.*

"

Le service FTP peut utiliser deux modes de communication possibles entre le serveur FTP et ses clients, à savoir le mode FTP passif et le mode FTP non passif.
Notez que tous les serveurs FTP ne prennent pas en charge les deux modes.

Fonctionnement du mode FTP non passif (ou traditionnel)

En mode FPT non passif, le client se connecte au serveur en créant un canal de contrôle. Pour chaque opération de données, le client indique au serveur de quelle manière il doit se connecter, en spécifiant les paramètres de la connexion de données (port de données, mode de transfert, type de représentation et structure). Le serveur utilise ensuite ces paramètres pour créer le canal de données.

Ce type de communication FTP est identique au modèle FTP spécifié dans le draft Internet standard pour FTP (RFC 959) et était auparavant couramment utilisé sur tous les réseaux TCP/IP.

Le mode FTP non passif est indispensable pour toutes les mises en œuvre du service FTP et est utilisé comme mode de communication par défaut par le service du proxy Web dans Microsoft Proxy Serveur versions 1.0 et 2.0.

Différences entre les modes FTP passif et non passif

Le mode FTP passif diffère du mode non passif par le fait que le client est chargé d'établir toutes les connexions au serveur, y compris la demande de connexion initiale ainsi que les autres connexions du canal de données. De cette façon, le mode FPT passif renforce la sécurité du client contre toute agression malveillante d'un serveur FTP.

Comme le mode FTP passif est utilisé sur plusieurs serveurs FTP récemment mis en œuvre sur Internet, Microsoft Proxy Serveur 2.0 fournit, par l'intermédiaire du registre Windows NT, le support permettant au service du proxy Web d'utiliser le mode FTP passif.
Il se peut néanmoins que vous deviez aussi prendre en charge le mode FTP passif pour les raisons suivantes :

* Vous utilisez un pare-feu qui ne peut pas autoriser les connexions entrantes à partir du serveur FTP.

* Vous utilisez des applications FTP tierces. Certaines applications s'avèrent plus faciles à configurer avec le mode FPT passif.

Pour activer la prise en charge de Proxy Serveur pour le mode FTP passif, vous devez modifier la clé de Registre suivante. Le nom, le type de données et les valeurs de l'entrée prises en charge sont énumérés ci-dessous :

NonPassiveFTPTransfer possède le type de données REG_DWORD.
Sa valeur par défaut est 1, ce qui signifie que le mode FTP Sendport (non passif) est utilisé comme mode de transfert par défaut pour le proxy FTP.

Si la valeur de l'entrée devient 0, le service du proxy Web prendra en charge le proxy FTP avec des serveurs utilisant le mode FTP. Dans le cas contraire, conservez la valeur 1 par défaut.

Cette entrée est installée par Proxy Serveur dans la clé de Registre Windows NT suivante :

HKEY_LOCALMACHINE\SYSTEM
\CurrentControlSet

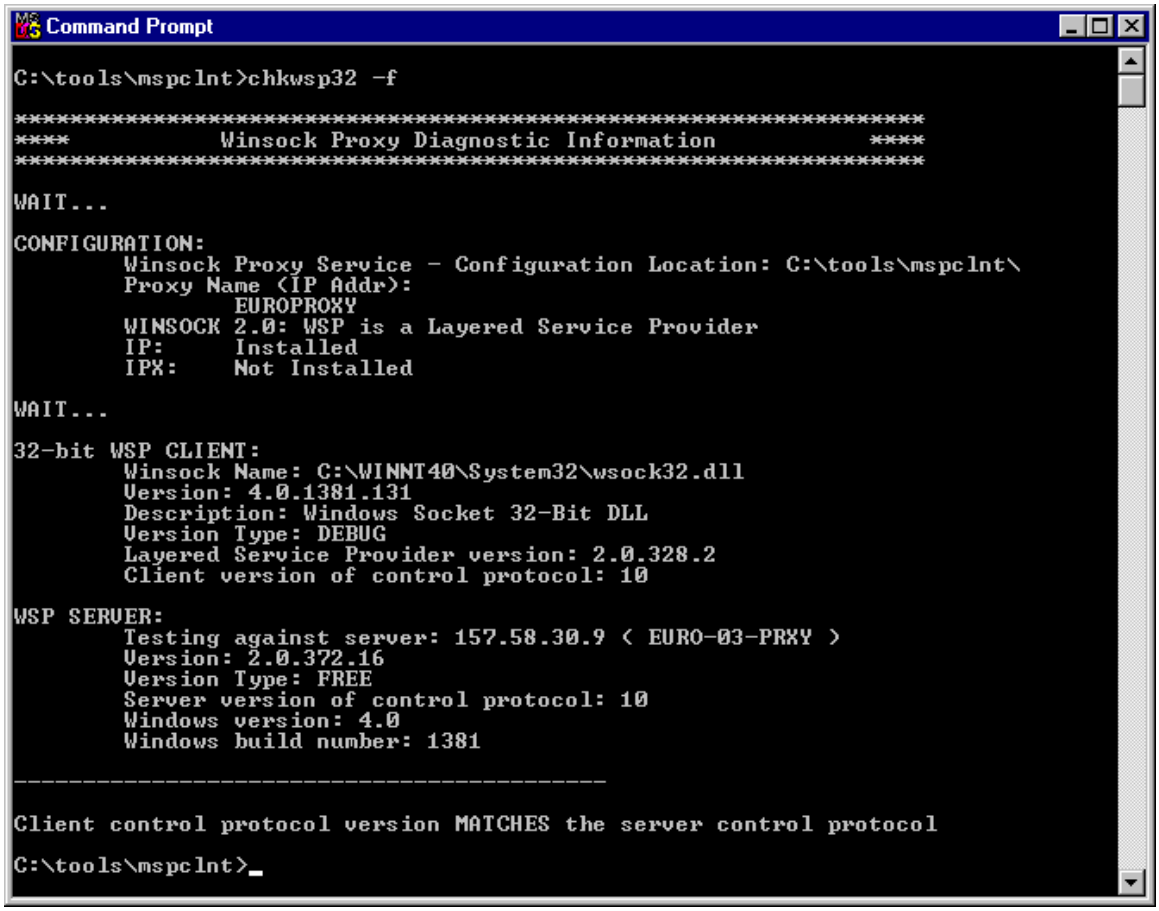
\Services
\W3proxy
\Parameters
"

7.2. Vérifier la connexion entre le client WSP et le serveur Proxy

Pendant l'installation du client est copié également dans le répertoire d'installation (par défaut c:\mspclnt) l'utilitaire CHKWSP32.
Pour déterminer tout problème de connexion entre le client WSP et le serveur Proxy un des premiers tests a faire est de lancer, depuis le client, à partir d'une console DOS, la commande:

chkwsp32 -f.

Cette commande va retourner quantité d'informations (version du client et du serveur, noms et adresses de machines, protocoles utilisés, etc...) et le résultat du test de la connexion. Si cette connexion réussit le message "Client control protocol matches the server control protocol" sera affiché.



Si la connexion échoue, le message d'erreur sera explicite:
"

- The configuration information is missing in the System.ini file in the [Microsoft Proxy Service] section, "Configuration Location" key.

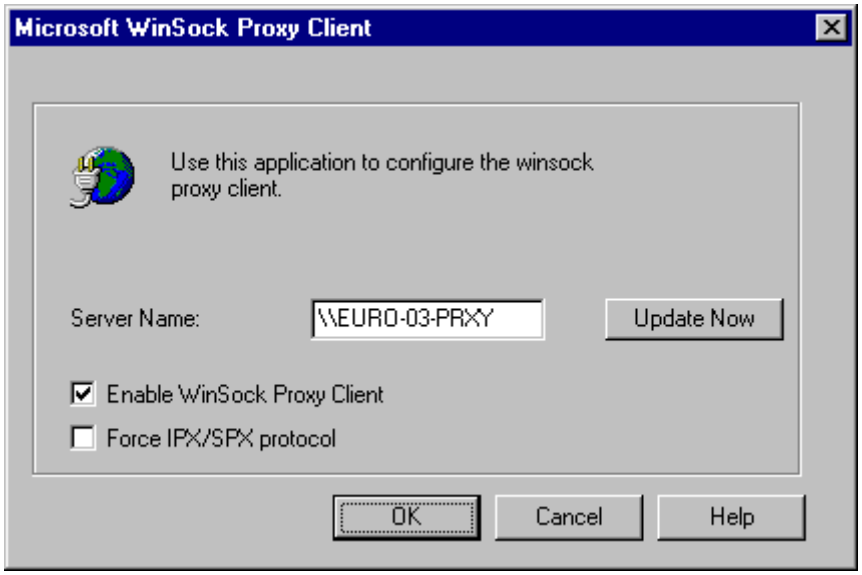
- The WinSock DLL was not found, or it was found to be the original system DLL rather than the one installed by the client Setup program. Check that you have only one copy of the WinSock DLL. It should be located in the Windows directory.
- *The WinSock Proxy service has denied client authentication.*

"

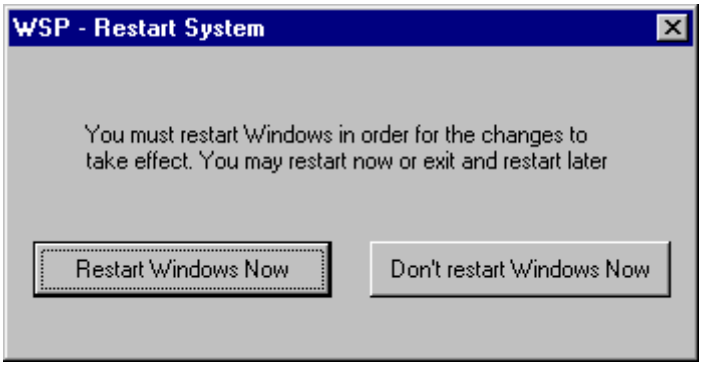
Dans le cas du dernier message, bien sur il est possible que le compte utilisé soit incorrect ou ait expiré, mais il faut également s'assurer que le compte n'a pas l'option "Le mot de passe peut expirer" de cochée: Si le mot de passe d'un compte NT peut expirer l'application Winsock ne fonctionnera pas à travers le service Winsock Proxy.

7.3. Mettre à jour les informations et la configuration du client

Le bouton "Update Now" qui se trouve sur l'interface de configuration du client Winsock proxy permet de mettre à jour les informations de ce client par rapport au serveur (MSPLAT.TXT et MSPCLNT.INI).



Il est nécessaire de redémarrer le poste client après cette mise à jour comme indique le message systématique qui suit:



Par contre, ce même message apparaît également systématiquement si le client est désactivé ou réactivé: **il n'est pas nécessaire de redémarrer le poste dans ce cas**.
La seule précaution à prendre est de fermer et relancer les applications Winsock (Telnet par exemple) après l'activation/désactivation du client WSP pour prendre en compte ce changement par les applications en question.

7.4. CREDTOOL

Supposons qu'un serveur Proxy fasse partie d'un Domaine A. Comment, depuis une machine d'un Domaine B, qui n'a aucune relation avec le Domaine A, mais en connaissant un compte utilisateur valable du Domaine A et son mot de passe, peut-on utiliser le service Winsock Proxy du serveur?

En effet, si l'installation du client WSP se fait facilement en utilisant le nom et mot de passe de l'utilisateur du domaine A pour se connecter sur le partage MSPCLNT du serveur, il n'en est pas de même pour faire fonctionner ce client. Car le compte d'authentification utilisé par le client WSP pour se connecter au serveur est celui de l'utilisateur logué sur la machine cliente...comment en configurer un spécifiquement?

C'est l'outil CREDTOOL qui permet cela.
CREDTOOL est également copié dans le répertoire d'installation du client WSP sur le poste.
"
CREDTOOL [-r|-w|-d] -n appname [-c User Domain Password]
-r reads the credentials
-w writes, or stores the credentials
-d deletes the credentials
-n appname specifies the name of the application executable file without the extension
-c user domain password specifies the account credentials
"

La procédure est la suivante:

a. dans le répertoire ou se trouve l'applicatif Winsock, créez un fichier WSPCFG.INI (avec notepad) demandant à l'applicatif de forcer une authentification spécifique:
"
```
[<nom de l'applicatif>]
ForceCredentials=1
```
"
Exemple, pour FTP, il faudra créer sous %SYSTEMROOT%\SYSTEM32 un WSPCFG.INI contenant:
"
```
[ftp]
ForceCredentials=1
```
"
b. lancez depuis une console DOS la commande suivante:
"
```
CREDTOOL -w -n <nom de l'applicatif> -c <username>
<domaine> <password>
```
"
Exemple:

"

CREDTOOL -w -n FTP -c lionelc southerneurope idic

"

7.5. Notions avancées

La plupart des applications Winsock n'ont pas besoin de configuration spéciale pour fonctionner avec le service Winsock Proxy. Il est toutefois possible de spécifier des paramètres spécifiques pour l'utilisation de ce service, paramètres qui peuvent être globaux ou spécifiques.

Les paramètres de configuration des applications sont enregistrés à deux endroits:

- **Le fichier de configuration globale du client: MSPCLNT.INI.** Il se trouve dans le répertoire d'installation du client WSP, sur le serveur donc. Ce fichier est mis à jour périodiquement depuis le serveur. En conséquence, le modifier sur le serveur permet de modifier la configuration automatiquement de tous les clients qui y sont rattachés. En contrepartie, il est inutile de modifier ce fichier sur les clients eux-mêmes car les données seront perdues à la prochaine mise à jour depuis le serveur.
  Dans ce fichier se trouvent les paramètres à appliquer a toutes les applications Winsock du client.
- **Le fichier de configuration d'application spécifique du client: WSPCFG.INI.** Il se situe dans le répertoire de l'application et n'est pas mis à jour par le serveur. Les informations qui s'y trouvent sont donc spécifiques à cette application de ce poste client.

Entre ces deux fichiers, comment sont lus les paramètres ?

L'algorithme est le suivant:

❖ L'application du client Winsock regarde d'abord dans son fichier MSPCLNT.INI (qui existe forcément). Là se trouvent des sections qui portent le nom des applications (une section par application).

❖ La première chose qu'elle regarde c'est le paramètre *Disable* dans la section [Common] du fichier MSPCLNT.INI. Si ce paramètre vaut 1, le service Winsock Proxy est désactivé.

❖ Sinon, elle cherche un fichier WSPCFG.INI dans son répertoire et, si ce fichier existe, elle regarde dans la section *[<nom de l'application WSP>]*. Si cette section n'existe pas, elle regarde dans la section *[Common]*. Si cette dernière n'existe pas non plus, elle regarde dans le même ordre ces sections dans le fichier MSPCLNT.INI. La première section trouvée dans cet ordre est la seule et unique qui sera utilisé pour spécifier les paramètres de cette application.

Pour résumer, l'ordre est donc:

1) la section *[<nom de l'application WSP>]* de WSPCFG.INI
2) la section *[Common]* de WSPCFG.INI
3) la section *[<nom de l'application WSP>]* de MSPCLNT.INI
4) la section *[Common]* de MSPCLNT.INI

Ci-après un exemple de section *[<nom de l'application WSP>]*:

"

[*WSP client*]
Disable=0
NameResolution=R
LocalBindTcpPorts=7777
LocalBindUdpPorts=7000–7022, 7100–7170
RemoteBindTcpPorts=30
RemoteBindUdpPorts=3000–3050
ServerBindTcpPorts=100–300
ProxyBindIp=80:110.52.144.103, 82:110.51.0.0
KillOldSession=1
Persistent=1
ForceProxy=i:172.23.23.23
ForceCredentials=1
NameResolutionForLocalHost=L

"

Le tableau suivant décrit les valeurs qui sont possibles de spécifier dans un fichier de configuration d'application Winsock cliente. Les entrées les plus couramment utilisées ont été soulignées:

Entry	***Description***
Disable	This setting disables the WinSock Proxy service for all WinSock Proxy client applications when the value is set to 1. In the *[Common Configuration]* section of the Mspclnt.ini file, this setting overrides any other settings.
NameResolution	By default, resolution for all dot-convention names is redirected. Forces name resolution to local (L) or redirected (R), as specified.
LocalBindTcpPorts	Specifies a TCP port, list, or range that is bound locally.
LocalBindUdpPorts	Specifies a UDP port, list, or range that is bound locally.
RemoteBindTcpPorts	Specifies a TCP port, list, or range that is bound remotely.
RemoteBindUdpPorts	Specifies a UDP port, list, or range that is bound remotely.
ServerBindTcpPorts	Specifies a TCP port, list, or range used by a server application, so an accept operation on these ports is intended to serve clients both locally and on the Internet. Requires that the port is available both on the client and the Proxy Server computer.
ProxyBindIp	Specifies an IP address or list that is used when binding with a corresponding port. Used by multiple servers that use the same port and need to bind to different ports on the Proxy Server computer. The syntax of the entry is: ***ProxyBindIp=****[port]* ***:*** *[IP address]****,*** *[port]* ***:*** *[IP address]*. The port numbers apply to both TCP and UDP ports.
KillOldSession	When the value is set to 1, this entry can be used to specify that if Proxy Server holds a session from an old instance of an application, that session is terminated before the application is granted a new session. This option solves the problem of restarting an application. For example, if an application crashed, or did not close the socket on which it was listening, it could have taken up to 10 minutes until Proxy Server discovered that the session for the application should have been terminated. At that time you would not have been able to

	restart the application because the port on which it was listening was already in use.
Persistent	When the value is set to 1, this entry can be used to maintain a specific server state on the Proxy Server if a service is stopped and restarted and if the server is not responding. The client sends a keep-alive message to the server periodically during an active session. If the server is not responding, the client tries to restore the state of the bound and listening sockets upon server restart.
ForceProxy	Used to force a specific Proxy Server computer for a specific Windows Sockets application. The syntax of the entry is: ***ForceProxy*=**[*tag*] ***:*** [*entry*], where *tag* equals ***i*** for an IP address, ***x*** for an IPX address, or ***n*** for a name. *Entry* is the address of the name. If the ***n*** flag is used, the WinSock Proxy service works over IP only.
ForceCredentials	Used when running a Windows NT service or server application as a WinSock Proxy client application. When the value is set to 1, forces the use of alternate user authentication credentials stored locally on the computer running the Windows NT service. The user credentials are stored on the client computer using the Credtool.exe application that is provided with Proxy Server. User credentials must reference a user account that can be authenticated by Proxy Server, either local to Proxy Server or in a domain trusted by Proxy Server. The user account is normally set not to expire; otherwise, user credentials need to be renewed each time the account expires.
NameResolutionForLocalHost	Used to specify how the "LocalHost" computer name is resolved. (The "LocalHost" computer name is resolved by calling the Windows Sockets API function gethostbyname() using the "LocalHost" string, an empty string, or a NULL string pointer.) This entry aids Windows Sockets applications that rely on the IP addresses that the local host computer resolves to. Such applications call gethostbyname("LocalHost") to find their local IP address and send it to an Internet server. When this option is set to ***L*** (the default), gethostbyname() returns the IP addresses of the local host computer. When this option is set to ***P***, gethostbyname() returns the IP addresses of the Proxy Server computer. When this option is set to ***E***, gethostbyname() returns only the external IP addresses of the Proxy Server computer (those IP addresses that are not in the LAT).

Remarque: Un seul port ne peut apparaître dans ces entrées. Il n'est pas possible d'avoir une application Web qui écoute à la fois sur le poste client et sur un port déporté. Pour des applications qui ont besoin d'être connectées à la fois sur le réseau interne et le réseau externe, il faudra faire diriger les connections interne également sur le Proxy.

8. Mettre en place de la sécurité d'accès

8.1. Internet Explorer prompte l'utilisateur anormalement

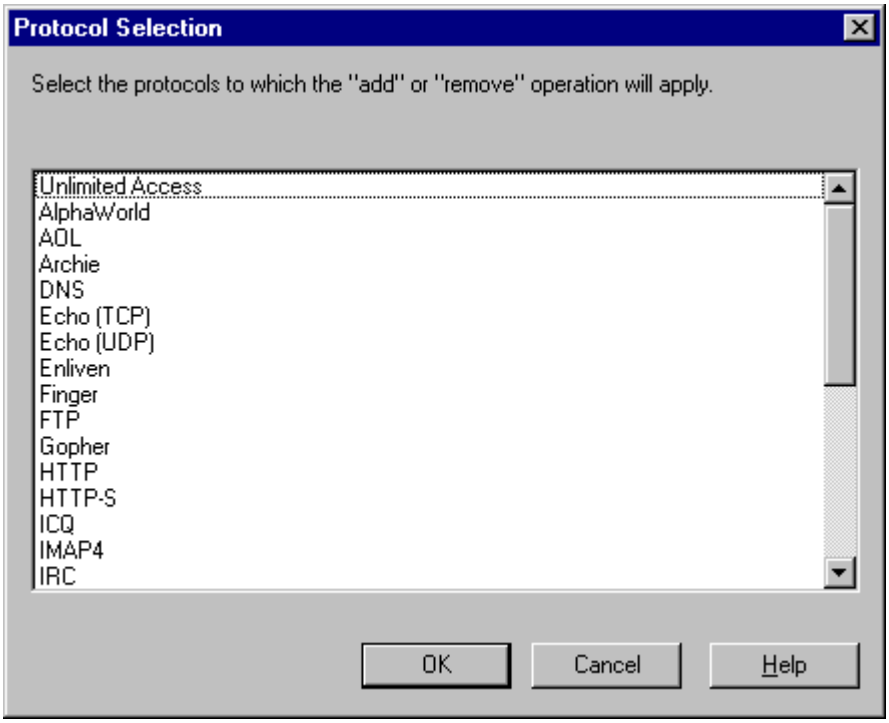
La fiche technique Q189033 explique qu'Internet Explorer jusqu'à sa version 4.01 SP1 incluse gère mal l'authentification avec un serveur Proxy en NTLM. Si une authentification est demandée alors qu'elle n'était pas attendue, il convient de regarder en premier lieu la version du browser et le cas échéant de le mettre à jour.

8.2. Définir des permissions pour un ou plusieurs protocoles

En plus du filtrage de domaine, il est possible de définir des permissions sur les protocoles associés à chaque service Proxy. Pour chacun des trois services, cette mise en place de permissions se fait via l'onglet "Permissions" des propriétés du service.

Remarque: En cas de résolution d'un problème quelconque avec Proxy Serveur, il est judicieux dans un premier temps de retirer tout filtrage de paquet, de domaine et toute permission pour déterminer si le problème a sa source dans l'installation, la connexion, la configuration ... ou si c'est la mise en place de la sécurité qui en est la cause.

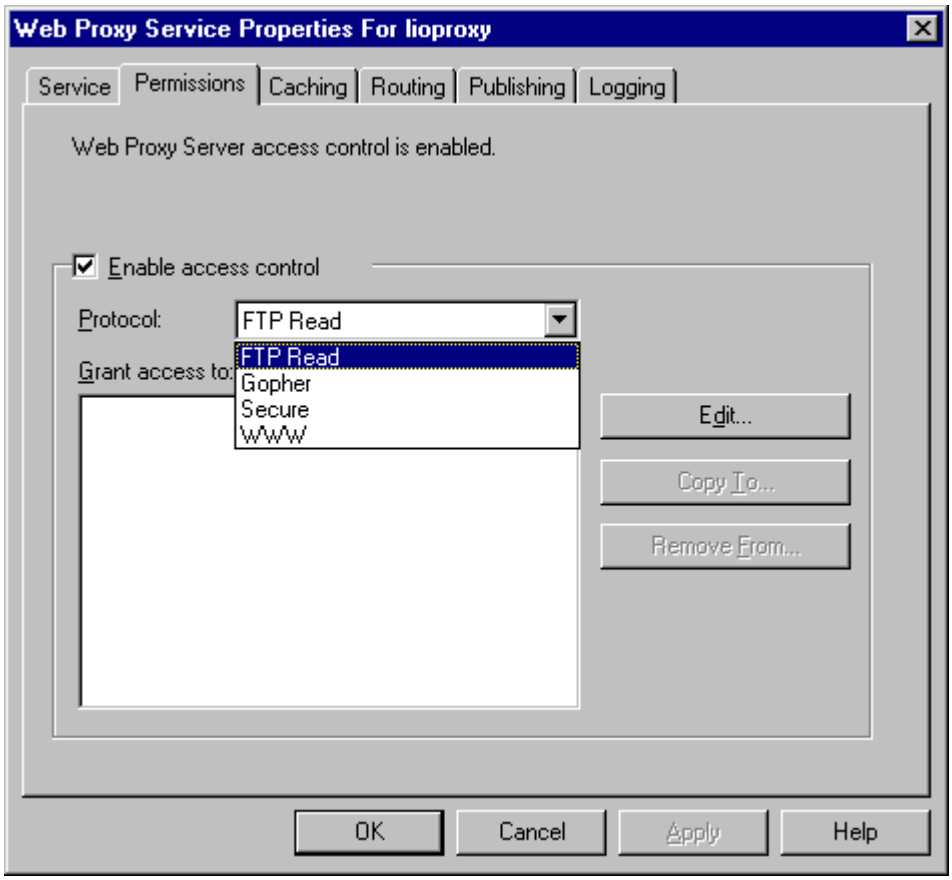
En utilisant l'interface il n'est possible de définir des permissions que pour UN protocole à la fois mais il est par contre possible de copier (ou supprimer) ces permissions à autant de protocoles désirés dans un second temps.



Remarques pour chacun des trois services:

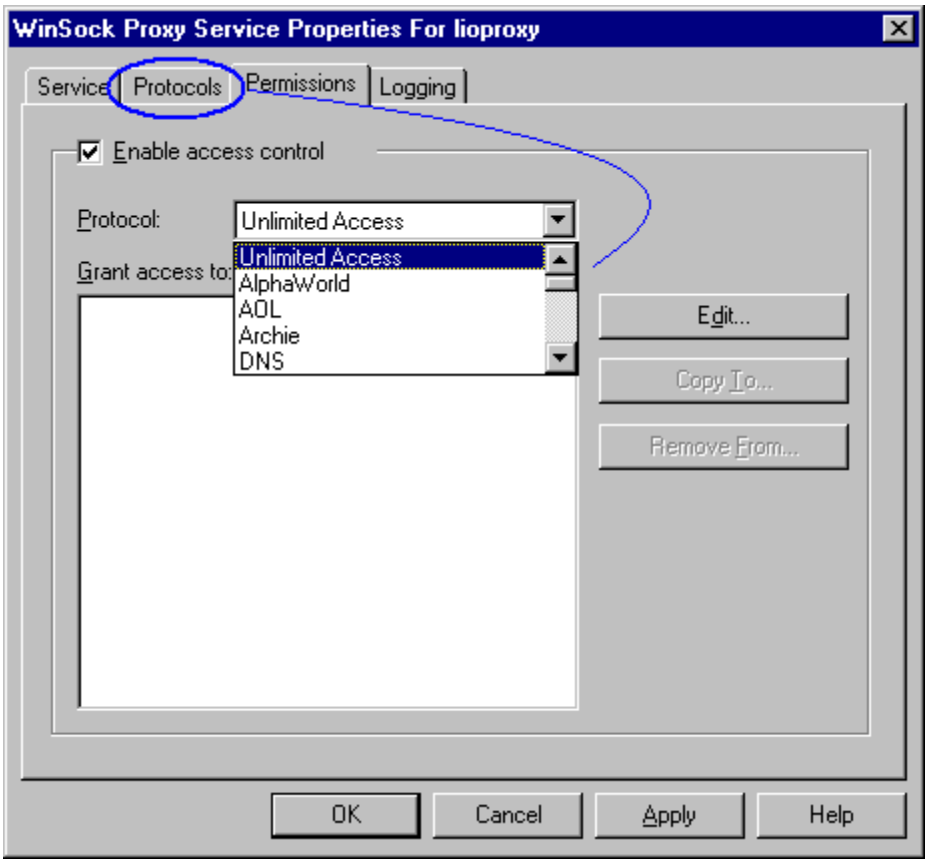
- Le service Web Proxy:

Les permissions utilisateur pour les protocoles HTTP et HTTPS sont identiques. Si vous affectez à certains utilisateurs des permissions pour le protocole WWW, ils auront accès aux pages Web SSL sécurisées (HTTPS) ainsi qu'aux pages Web HTTP standard. Les utilisateurs n'ayant pas les permissions requises pour le protocole WWW n'auront accès ni au protocole HTTP ni au protocole HTTPS.



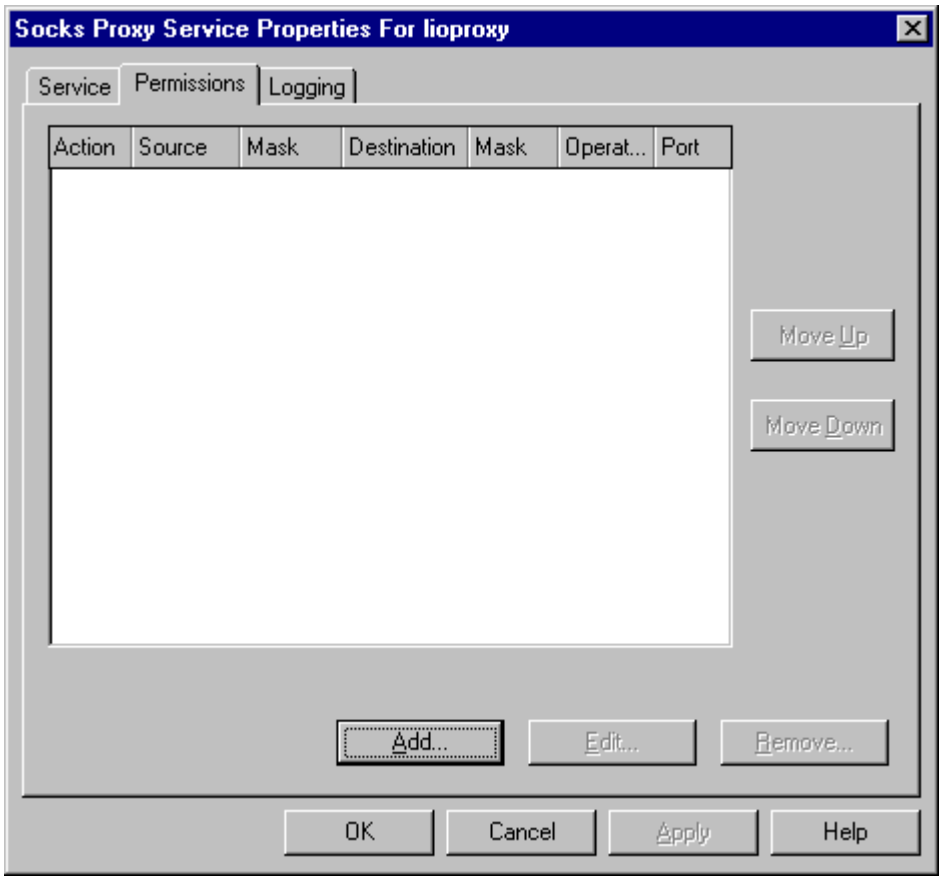
❑ Le service Winsock Proxy:

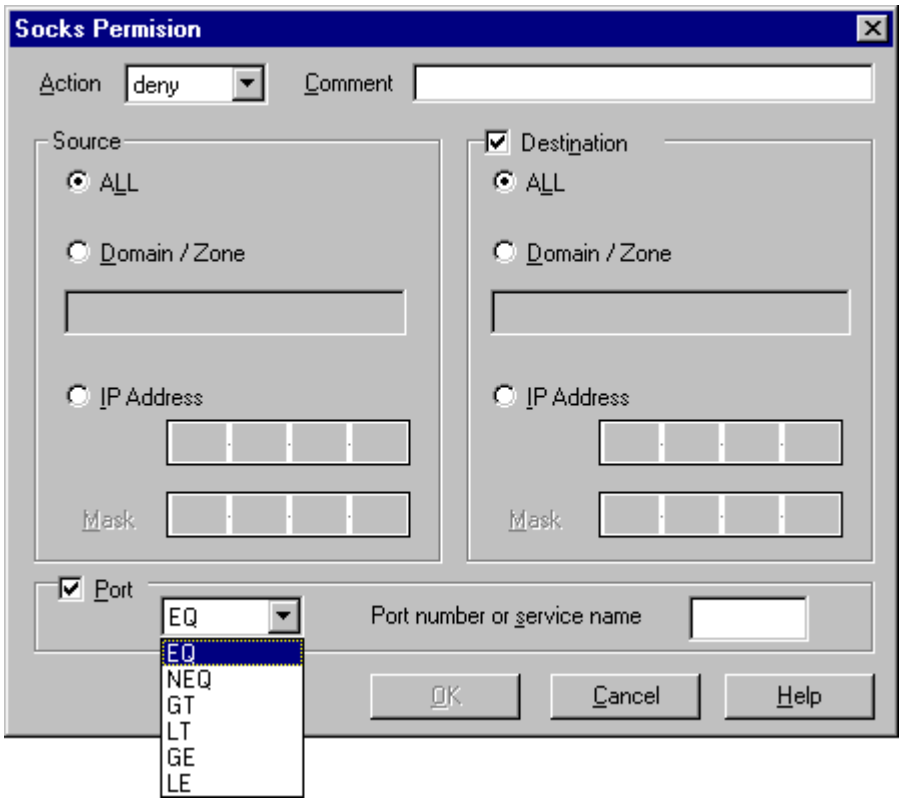
Il y a des protocoles définis par défaut mais on peut définir les siens propres et leur affecter des permissions au même titre.
Attention au droit "Unlimited Access".



❑ Le service SOCKS Proxy:

Les permissions y sont particulières car elles ne s'appuient pas sur les utilisateurs de la machine mais sur des notions d'adresses IP et de port.


Socks Proxy Service Properties For lioproxy
Service
Permissions
Logging
Action
Source
Mask
Destination
Mask
Operat...
Port
Move Up
Move Down
Add...
Edit...
Remove...
OK
Cancel
Apply
Help


Socks Permision
Action
deny
Comment
Source
ALL
Domain / Zone
IP Address
Mask
Destination
ALL
Domain / Zone
IP Address
Mask
Port
EQ
Port number or service name
EQ
NEQ
GT
LT
GE
LE
OK
Cancel
Help

8.3. Spécifier un compte à la connexion

Gardez à l'esprit, pour tester vos permissions, qu'il est possible de spécifier un compte sans avoir à se reloguer:

- **Pour le Web Proxy:** (RFC 1738)
  http://<Utilisateur>:<mot de passe>@<Serveur>:<Port>/<page HTML>

  Exemple:
  "
  http://lionelc:idic@Ariane:80/Ariane98/default.asp
  "
- **Pour le Winsock Proxy:** avec CREDTOOL (voir plus haut)
- **Pour le SOCKS Proxy:** cela dépend de l'application SOCKS...

8.4. Le serveur Proxy et les permissions des serveurs Web

Gardez également à l'esprit que le mode "Stimulation/Réponse" ne passe pas à travers un serveur Proxy. Les seules méthodes d'authentifications sur un serveur Web à travers un serveur Proxy sont: Anonyme, Authentification Texte Clair, par cookies, par formulaire HTML ou par Certificats (ou d'autres, via des clients spécifiques)
Pour plus de détails, consultez l'article Q198116.

9. Déployer les clients

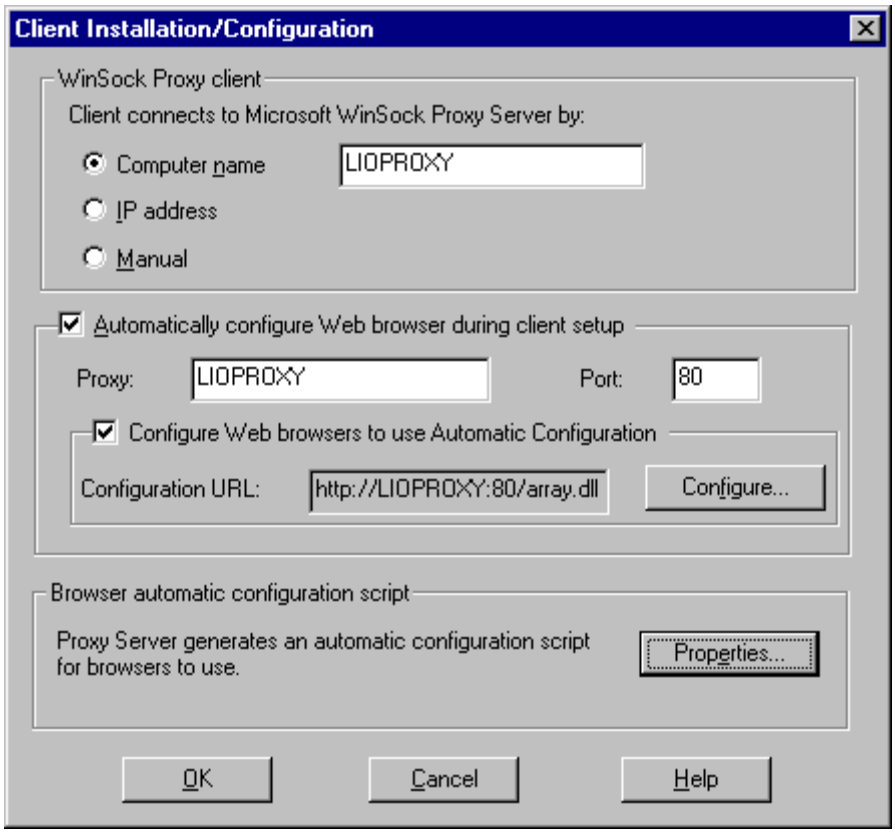
9.1. Déployer l'installation

- **Pour utiliser le service Web Proxy:** pour cela il est juste nécessaire d'avoir un browser sur les postes. Un tel déploiement peut s'envisager pour ce qui est d'Internet Explorer en utilisant l'Internet Explorer Administration Kit (IEAK). http://www.microsoft.com/windows/ieak
- **Pour utiliser le service Winsock Proxy:** nous avons vu qu'il était possible d'installer le client WSP en ligne de commande et de manière Automatique (Unattended). En conséquence, il est possible d'installer WSP par un logon script ou via SMS.
  Il est également envisageable de rajouter le client WSP comme un composant à déployer avec l'installation de IE en passant par l'IEAK.
- **Pour utiliser le service SOCKS Proxy:** il n'y a pas de client SOCKS, il faut par contre s'assurer que l'application cliente SOCKS est configurable pour utiliser un serveur SOCKS Proxy et est compatible avec le serveur Microsoft Proxy (voir chapitre 5.2).

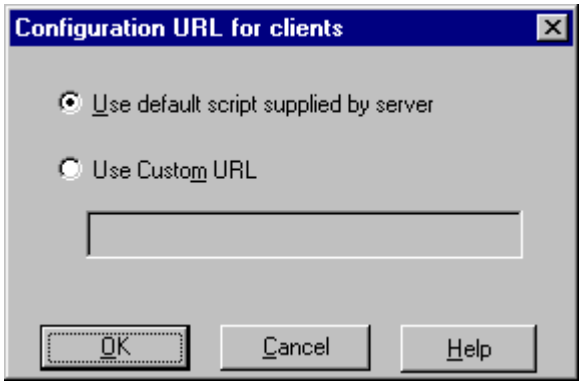
9.2. Déployer la configuration

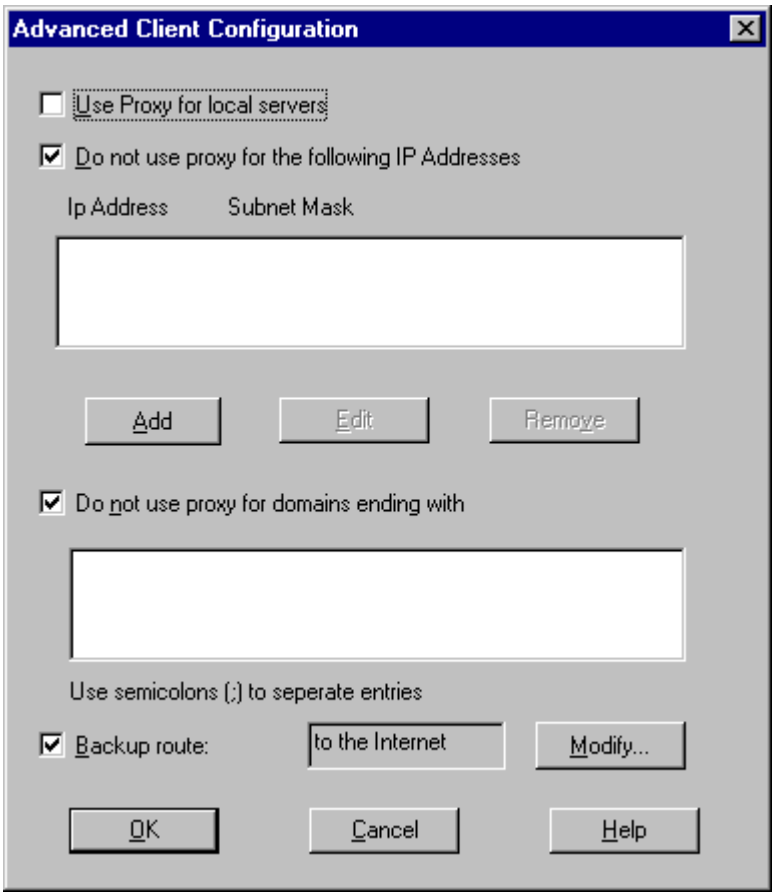
Nous avons déjà vu que la mise à jour du fichier MSPCLNT.INI était automatique, ceci constitue un moyen de déploiement de configuration du client WSP.

De plus, comme l'installation du WSP est effectuée à partir d'un partage du serveur, il est possible de spécifier dans l'interface du serveur des options de paramétrage du client et plus spécifiquement du browser du poste sur lequel WSP va être installé.



Le Script de configuration automatique (généré par défaut par la bibliothèque Array.dll par l'URL: http://<Serveur Proxy>:80/array.dll?Get.Routing.Script), est en fait un fichier .pac renvoyé au browser. C'est un script JavaScript qui est chargé en mémoire sur le poste du browser (et non pas sur le disque) à chaque démarrage du browser.





Ce fichier permet au browser:

- de savoir quelles sont les URLs pour lesquelles il faut contacter le serveur Proxy ou pas
- quel Serveur Proxy contacter suivant l'URL demandée
- si le Proxy est un tableau de serveurs Proxy, quel membre de ce tableau contacter en priorité suivant l'URL demandée (le serveur qui a le plus de chance de posséder dans son cache l'URL en question)

Le premier point est donc un moyen de configurer le poste client de manière centralisée; dans le script se trouve une fonction au nom normalisé: FindProxyForURL(url, host) qui peut indiquer entre autre des URLs pour lesquelles il faut contacter un serveur Proxy ou au contraire résoudre localement.

```
function FindProxyForURL(url, host)
{
        if (isPlainHostName(host))
                return "DIRECT";
        else if (shExpMatch(host, "msdn.microsoft.com"))
                return "PROXY EUROPROXY:80";
        else if (shExpMatch(host, "*.microsoft.com"))
                return "DIRECT";
        else
                return "PROXY EUROPROXY";
}
```

Les deux autres points sont relatifs au fait d'avoir plusieurs serveurs Proxy, sujet que nous abordons dans le prochain chapitre...

10. Mettre en place plusieurs serveurs Proxy si nécessaire

10.1. Le script de configuration automatique

L'exécution de ce fichier renvoie (par l'intermédiaire de la fonction FindProxyForURL(url, host)) une chaîne du type:

```
PROXY EUROPROXY:8080; PROXY mon.serveur.proxy:8081
```

Il est donc possible, par l'intermédiaire de ces fichiers, non seulement d'indiquer si la demande d'une URL bien précise doit être résolue localement ou pas, mais dans ce dernier cas, vers quel serveur la transmettre et les autres solutions si ce dernier serveur ne répond pas.
Dans l'exemple précédent la chaîne indique que pour atteindre l'URL demandée il faut passer en premier lieu via EUROPROXY mais que si ce dernier ne répond pas alors de transmettre la requête à mon.serveur.proxy sur le port 8081.

Le critère de sélection d'un serveur ou un autre peut être basé sur quantité d'éléments. On peut imaginer par exemple la fonction suivante qui distingue les serveurs Proxy à utiliser suivant le protocole demandé:

```
function FindProxyForURL(url, host)
{
      if (url.substring(0, 5) == "http:") {
        return "PROXY proxy:80";
        }
      else if (url.substring(0, 4) == "ftp:") {
        return "PROXY fproxy:80";
        }
      else if (url.substring(0, 7) == "gopher:") {
        return "PROXY gproxy";
        }
      else if (url.substring(0, 6) == "https:") {
        return "PROXY secproxy:8080";
        }
      else {
        return "DIRECT";
        }
}
```

Par contre, il n'est pas possible de spécifier l'utilisation de tel ou tel Proxy suivant le compte utilisateur employé. Ceci est une demande classique que seules l'utilisation de .pac spécifiques par utilisateur ou l'installation d'add-on à Proxy Serveur http://www.microsoft.com/proxy/showcase/Filter.asp?A=3&B=3 peut rendre possible.

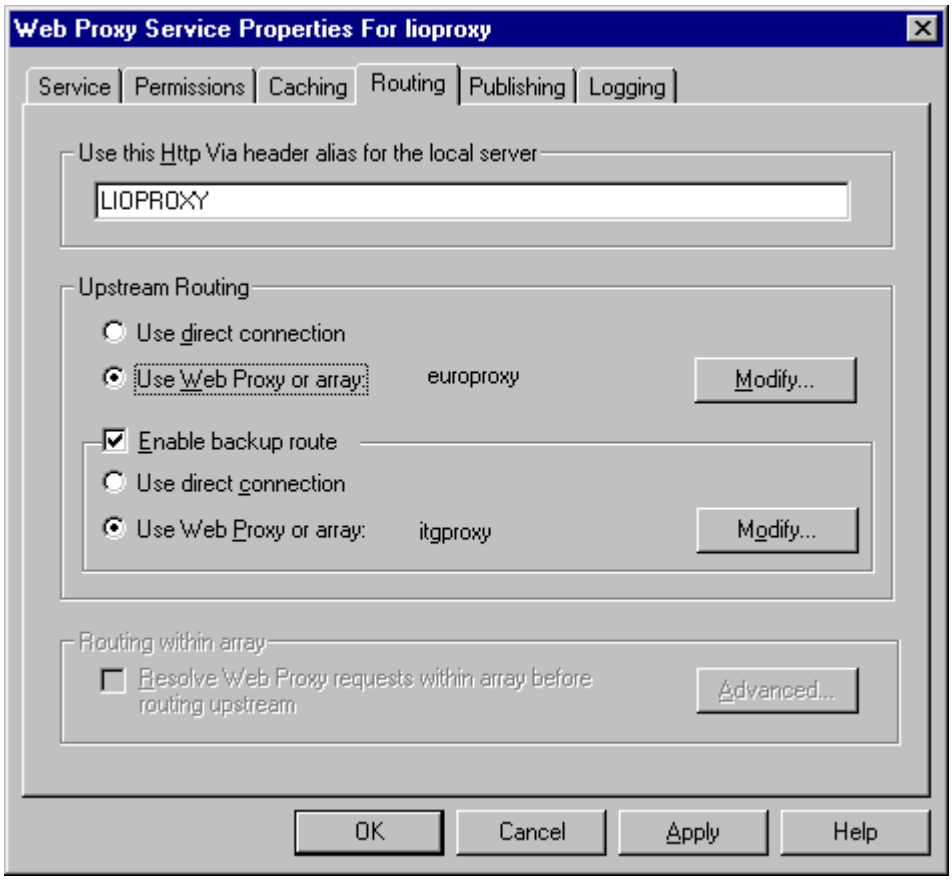
Remarque: en plus des mots clés DIRECT et PROXY il est possible d'employer le mot SOCKS pour indiquer un serveur SOCKS.

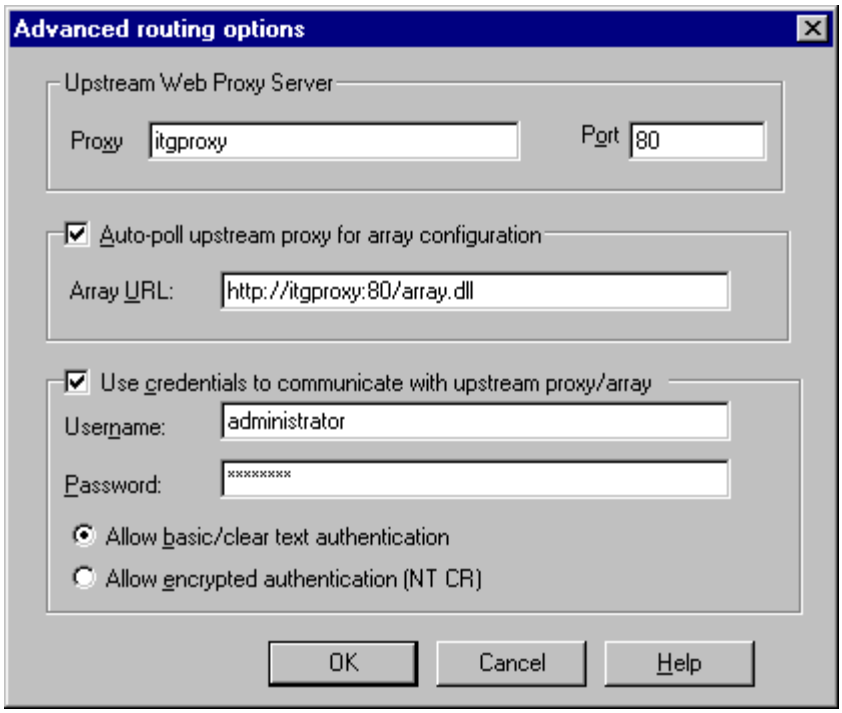
10.2. Les chaînes de Proxy

Il est possible de chaîner des Serveurs Proxy. Cette fonctionnalité permet par exemple d'avoir un Serveur Proxy local et, si l'URL demandée n'est pas présente

dans le cache local, transmettre cette requête à un serveur Proxy "au-dessus", le serveur d'une agence centrale ou d'un ISP par exemple.

Le chaînage de serveurs est un chaînage pour le service Web Proxy uniquement, il n'est pas possible de faire du chaînage de requêtes Winsock ou SOCKS.





Attention: lorsque de telles chaînes sont mises en place, la sécurité de la chaîne dans sa globalité est à reconsidérer. L'apparition du correctif décrit dans l'article Q231349 a modifié le comportement d'une chaîne en terme de sécurité:

1er cas: Les serveurs n'ont pas le SP1 (ni le hotfix)
Ceci est donc valable pour toute machine sur IIS3.0 ou les machines IIS4 sans le hotfix ou le SP1.
Dans ce cas, si un client a les tous les droits nécessaires pour effectuer une requête sur un serveur Proxy, sa requête va être satisfaite même si elle est transmise à un serveur plus haut dans la chaîne pour être résolue et que l'utilisateur ne dispose pas des droits sur ce serveur.
En fait, si le serveur upstream a de la sécurité mise en place et qu'il demande une authentification au serveur downstream, ce dernier répondra par le compte spécifié dans l'interface de routage Web Proxy et non l'authentification du client final.
Conclusion: Des utilisateurs n'ayant pas le droit d'utiliser des ressources d'un serveur Proxy peuvent donc arriver a contourner cette interdiction en passant par un serveur downstream.

2ème cas: Les serveurs disposent du SP1 (ou le hotfix)
En cas de demande d'authentification d'un serveur upstream, le serveur downstream ne répondra pas par le compte spécifié dans l'interface de routage Web Proxy mais transmettra la demande au client Web final.
Nous sommes donc dans le cas ou un serveur Proxy va devoir transmettre une demande d'authentification et dans ce cas NTLM ne peut donc être utilisé, cette méthode ne supportant pas la délégation.
"

What the Fix Does

With this fix applied, Proxy Server checks an additional registry entry type DWORD in "HKLM\System\CurrentControlSet\Services\W3Proxy\Parameters" named

"PassThroughAuth." If the "PassThroughAuth" value is set to 0x01, the Web Proxy forwards 407 "Proxy-Authenticate" responses from the upstream Web Proxy to the client.

Therefore, a logon dialog pops up at the client asking for credentials if basic authentication is used on the upstream Web Proxy. This does not work if NTLM authentication is used on the upstream Web Proxy because NTLM authentication cannot be delegated.

CAUTION: Using this additional Web Proxy feature may introduce a security risk if caching is enabled on the downstream Web Proxy. This is because clients connected to the downstream Web Proxy are able to retrieve files from the Web Proxy cache pulled through the upstream Web Proxy without first authenticating with the upstream Web Proxy.
"

Conclusion: Si la mise en place de sécurité est nécessaire sur un serveur upstream, la seule méthode d'authentification possible est l'authentification en texte clair.

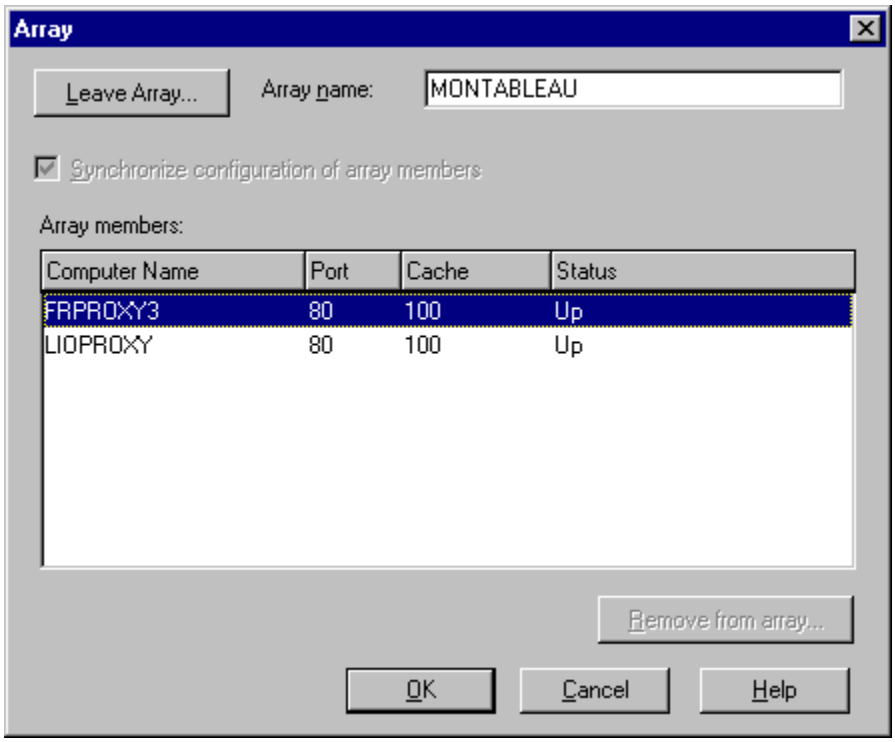
Remarque: La limitation ainsi mise en évidence par NTLM ne s'applique pas pour de l'authentification entre serveurs Proxy, il n'est plus question en effet dans ce cas de délégation.

10.3. Les tableaux de Proxy

a) La mise en place

Pour former un tableau (Array) de serveurs Proxy il est nécessaire que:
- les membres du tableau (nœuds) ont tous deux cartes
- toutes les cartes externes et toutes les cartes internes et ont la même configuration
- les cartes externes sont toutes connectées sur le monde extérieur (Routeur/FireWall vers Internet)
- les cartes internes sont toutes sur le réseau interne

Les browsers sont alors à configurer avec un proxy qui est le nom de l'array.



La librairie Array.dll permet également d'avoir le statut sur les serveurs du tableau par la commande Get.Info.v1. Cette fonction renvoie une ligne pour chaque serveur formatée suivant le modèle:

"

<Server Name> <IP @> <Port N°> <URL of array.dll> <Version of MSP> <how many seconds has been in the current state> <Up/Down> <Load Factor> <Cache size>

"

Exemple:

http://itgproxy:80/array.dll?Get.Info.v1

Renvoie:

"

Proxy Array Information/1.0
ArrayEnabled: 1
ConfigID: 921523764
ArrayName: ITGPROXY
ListTTL: 3000

RED-PRXY-01 157.54.9.71 80 http://RED-PRXY-01:80/array.dll MSProxy/2.0 28696 Up 100 18000
RED-PRXY-02 157.54.9.72 80 http://RED-PRXY-02:80/array.dll MSProxy/2.0 302444 Up 100 18000
RED-PRXY-03 157.54.9.73 80 http://RED-PRXY-03:80/array.dll MSProxy/2.0 28336 Up 100 18000
RED-PRXY-04 157.54.9.74 80 http://RED-PRXY-04:80/array.dll MSProxy/2.0 28576 Up 100 18000
RED-PRXY-05 157.54.9.75 80 http://RED-PRXY-05:80/array.dll MSProxy/2.0 28576 Up 100 18000
RED-PRXY-06 157.54.9.76 80 http://RED-PRXY-06:80/array.dll MSProxy/2.0 28336 Up 100 18000
RED-PRXY-07 157.54.9.77 80 http://RED-PRXY-07:80/array.dll MSProxy/2.0 28576 Up 100 18000
RED-PRXY-08 157.54.9.78 80 http://RED-PRXY-08:80/array.dll MSProxy/2.0 28336 Up 100 18000
RED-PRXY-09 157.54.9.79 80 http://RED-PRXY-09:80/array.dll MSProxy/2.0 28456 Up 100 18000
RED-PRXY-10 157.54.9.70 80 http://RED-PRXY-10:80/array.dll MSProxy/2.0 28216 Up 100 18000

"

Remarque: Toutes les communications qui ont lieu entre les membres d'un tableau sont via HTTP. Par contre RPC est nécessaire pour mettre en place le tableau, il n'est ensuite plus utilisé.

Les deux avantages de disposer d'un tableau de serveurs Proxy sont:
- La répartion du cache Web Proxy sur plusieurs machines et le protocole CARP
- La tolérance de panne

b) Le protocole CARP

Il existe un White Paper présentant ce protocole et comment il est géré. En résumé, le cache Web proxy étant réparti sur plusieurs machines, ce protocole permet de gérer efficacement cette répartition en permettant au browser de déterminer quel est le serveur membre du tableau qui a le plus de probabilité de contenir dans son cache l'URL demandée.
Ce calcul statistique de la part du client est inclus dans le fichier d'AutoConfiguration par défaut généré par les serveurs Proxy de ce tableau dont voici un exemple:
"

```
//Copyright (c) 1997 Microsoft Corporation
BackupRoute="DIRECT";
UseDirectForLocal=true;
cDirectIPs=0;
cDirectNames=0;
cNodes=2;
function MakeProxies(){
this[0]=new Node("FRPROXY3:80",3998418777,1.000000);
this[1]=new Node("LIOPROXY:80",3548866149,1.000000);
}
Proxies = new MakeProxies();
function Node(name, hash, load){
 this.name = name;
 this.hash = hash;
 this.load = load;
 this.score = 0;
 return this;
}
function FindProxyForURL(url, host){
 var urlhash, ibest, bestscore, list, i, j;
 if (UseDirectForLocal && isPlainHostName(host))
  return "DIRECT";
 if (cDirectNames > 0)
  for (i = 0; i < cDirectNames; i++)
   if (dnsDomainIs(host, DirectNames[i]))
    return "DIRECT";
 if (cDirectIPs > 0)
  for (i = 0; i < cDirectIPs; i += 2)
   if (isInNet(host, DirectIPs[i], DirectIPs[i+1]))
    return "DIRECT";
 urlhash = HashString(url);
 for (i = 0; i < cNodes; i++)
  Proxies[i].score = Proxies[i].load * Scramble(MakeInt(urlhash ^
Proxies[i].hash));
 list = "";
 for (j = 0; j < cNodes; j++) {
  for (bestscore = -1, i = 0; i < cNodes; i++) {
```

```
          if (Proxies[i].score > bestscore) {
           bestscore = Proxies[i].score;
           ibest = i;
          }
         }
         Proxies[ibest].score = -1;
         list = list + "PROXY " + Proxies[ibest].name + "; ";
        }
        list = list + BackupRoute;
        return list;
       }
       function HashString(url){
        var h = 0;
        var slashes = 0;
        for (var i = 0; i < url.length; i++) {
         var c = url.charAt(i);
         if (c == '/')
          slashes++;
         if (slashes < 3)
          c = c.toLowerCase();
         h += (((h & 0x1fff) << 19) | ((h >> 13) & 0x7ffff)) +
       CharToAscii(c);
         h = MakeInt(h);
        }
        return h;
       }
       function Scramble(h){
        h += ((h & 0xffff) * 0x1965) + ((((h >> 16) & 0xffff) * 0x1965)
       << 16) + (((h & 0xffff) * 0x6253) << 16);
        h = MakeInt(h);
        h += (((h & 0x7ff) << 21) | ((h >> 11) & 0x1fffff));
        return MakeInt(h);
       }
       var Chars =" !\"#$%&\'()*+,-
       ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]^_`abcdefghijklm
       nopqrstuvwxyz{|}~ € ??????????? Ž  ??????????? ž? ¡¢£¤¥¦§¨©ª«¬-®
       ¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîï
       ðñòóôõö÷øùúûüýþ";
       function CharToAscii(c){
        return Chars.indexOf(c) + 32;
       }
       function MakeInt(x){
        if (x < 0) {
         return x + 4294967296;
        } else if (x >= 4294967296) {
         return x - 4294967296;
        }
        return x;
       }
"
```

C'est la fonction HashString(url) qui permet au browser, à partir de l'URL demandée, de déterminer quel est le membre du tableau qui a le plus de chance d'avoir mis dans son cache cette URL...

c) La tolérance de pannes

Si un membre du tableau n'est plus disponible, les membres de ce tableau s'en aperçoivent (il y a un "poll" fréquemment) et ne contactent plus ce serveur ni ne tentent de faire appel a son cache Web jusqu'à ce que ce serveur redevienne disponible: c'est la fonctionnalité de tolérance de panne standard incluse avec le produit.

Il y a un problème: le premier serveur sur lequel est créé le tableau (attention: ce n'est pas le serveur à partir DUQUEL on spécifie le nom du tableau) est particulier, c'est le serveur Primaire. La principale conséquence réside dans le fait que toutes les machines sur lesquelles va être installé le client WSP vont se retrouver avec une URL spécifiant le script d'AutoConfiguration qui pointe sur ce serveur.

Du coup tous les browsers vont chercher leur script sur le même serveur ce qui pose des problèmes de goulot d'étranglement et de "single point of failure". Donc, avec un tableau, il est classique de configurer les browsers avec une URL de configuration automatique qui pointe sur une adresse du style:
http://<Un nom de A record dans un DNS>:80/array.dll?Get.Routing.Script
Il faut ensuite configurer les postes clients pour utiliser un serveur DNS sur lequel est enregistré des alias (CNAME) sur ce A record pointant sur les membres de mon tableau. Ce qui nous permet d'utiliser le round robin de DNS...

MAIS le round robin va donc déterminer de manière aléatoire quel serveur Proxy contacter... ce qui entre en conflit avec le protocole CARP qui est plus à même de faire ce choix...

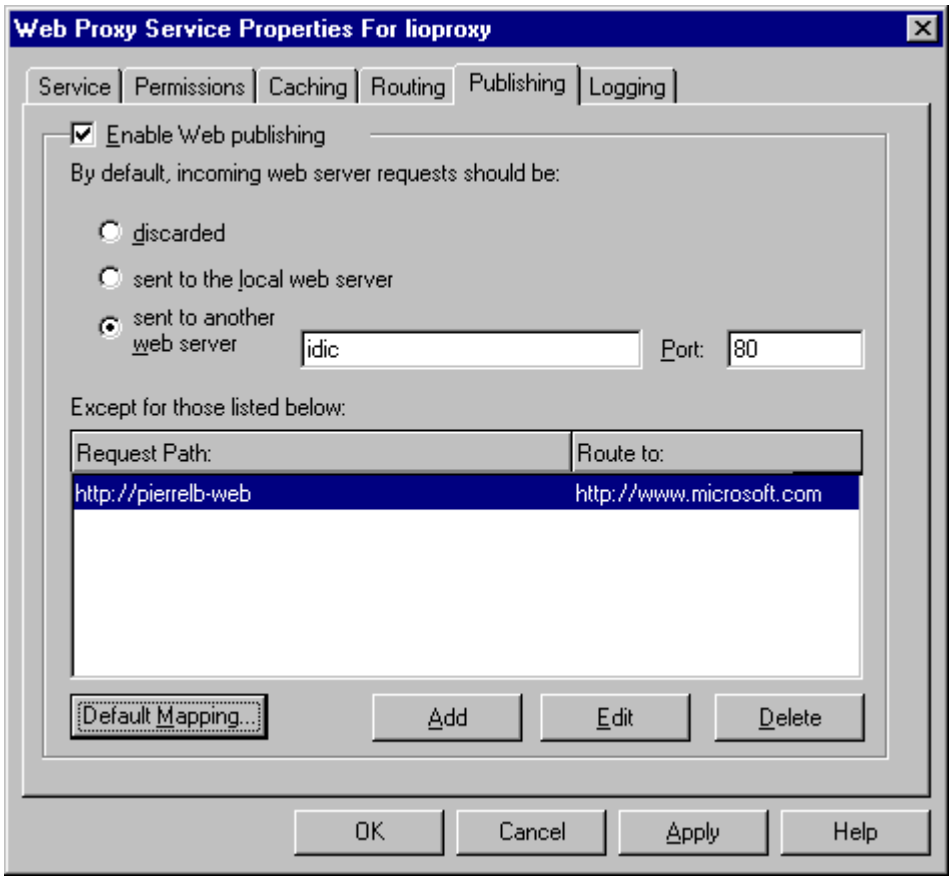
Remplacer le "DNS round robin" par WLBS (Windows Load Balancing Service) pose le même inconvénient. WLBS par contre étant plus adapté que le round robin pour ce qui est de la tolérance de panne Winsock ou SOCKS son emploi est donc préférable, mais l'intérêt du protocole CARP est tout de même perdu.

Conclusion: Proxy Serveur n'étant pas "Cluster Aware", il n'existe pas de solution complète de tolérance de panne permettant de conserver l'intérêt du protocole CARP.

11. Intégrer Proxy avec des services et des serveurs existants

11.1. Le "Web Publishing"

La fonctionnalité de "Web Publishing" permet de gérer une liste des serveurs Web internes qui ont la permission de publier sur l'Internet. De ce fait, le serveur Proxy se met à écouter les requêtes Internet, chose qu'il rejette par défaut à l'installation, et soit les gère localement soit les retransmet à d'autres serveurs internes.



Ceci ne fonctionne que pour HTTP et pas pour FTP ou GOPHER.

Il est fortement recommandé que le serveur Web sur lequel les requêtes sont transmises ne soit pas le serveur Proxy lui-même mais bien sur une machine tierce de mon intranet. Ceci pour:

- ne pas ajouter à la charge du serveur Proxy le rôle d'un serveur Web
- gérer la sécurité du serveur Web indépendamment de celle du serveur Proxy.

Activer de l'authentification sur un serveur Proxy qui écoute pour le compte de serveurs Web internes n'est pas recommandé. En effet, le fait de passer à travers un Proxy doit être transparent pour tout utilisateur d'un serveur Web.
De plus, si de l'authentification est mise en place sur un serveur Proxy, c'est la même authentification qui va être utilisée pour le serveur Web (il y a une seule entête dans une requête HTTP) et donc il faudra calquer l'authentification du serveur Proxy sur le serveur Web (comptes homonymes avec même mot de passe, etc...) ce

qui enlève de la liberté de gestion (et dans ce cas là, seule l'authentification en texte clair car c'est la seule qui support la délégation).

Microsoft recommande que seul l'accès anonyme soit validé sur le service WWW d'un serveur Proxy faisant du Web Publishing que le service Web Proxy ait un contrôle d'accès activé ou pas.

Lors de la mise en place du Web Publishing, il convient de s'assurer que:
- si le filtrage de paquets est activé, les ports nécessaires au protocole HTTP ou HTTPS soient autorisés
- si le Web publishing route les requêtes vers un serveur intranet, le nom de ce serveur (L'URL de redirection) soit résolvable par le serveur Proxy, si ce n'est pas le cas, il faudra spécifier l'adresse IP
- le SP1 soit mis en place sinon des délais de réponse de l'ordre d'une minute sont à prévoir (Q191414) et toute requête sur une URL de 78 ou 79 caractères échouera (Q225342)
- Le NOM du serveur Web a atteindre doit être associé à l'adresse IP du serveur Proxy dans le serveur DNS qui référence le site sur Internet.

Utiliser SSL avec le Web Publishing:
Il n'est pas vraiment possible d'utiliser SSL à travers le serveur Proxy de manière immédiate, il faut soit envisager de limiter HTTPS entre le client et le serveur Proxy et faire de l'HTTP entre le proxy et le serveur Web, soit utiliser HTTPS entre le client et le Proxy et entre le Proxy et le serveur Web mais ces deux communications étant basées sur des certificats différents.
Pour faire du SSL entre un client et un serveur Web via un Proxy, il faut déporter le port d'écoute HTTPS du serveur Web sur le serveur Proxy (voir chapitre 11.3.). Cette manipulation est décrite dans la fiche Q184030.

11.2. Mettre en place une DMZ

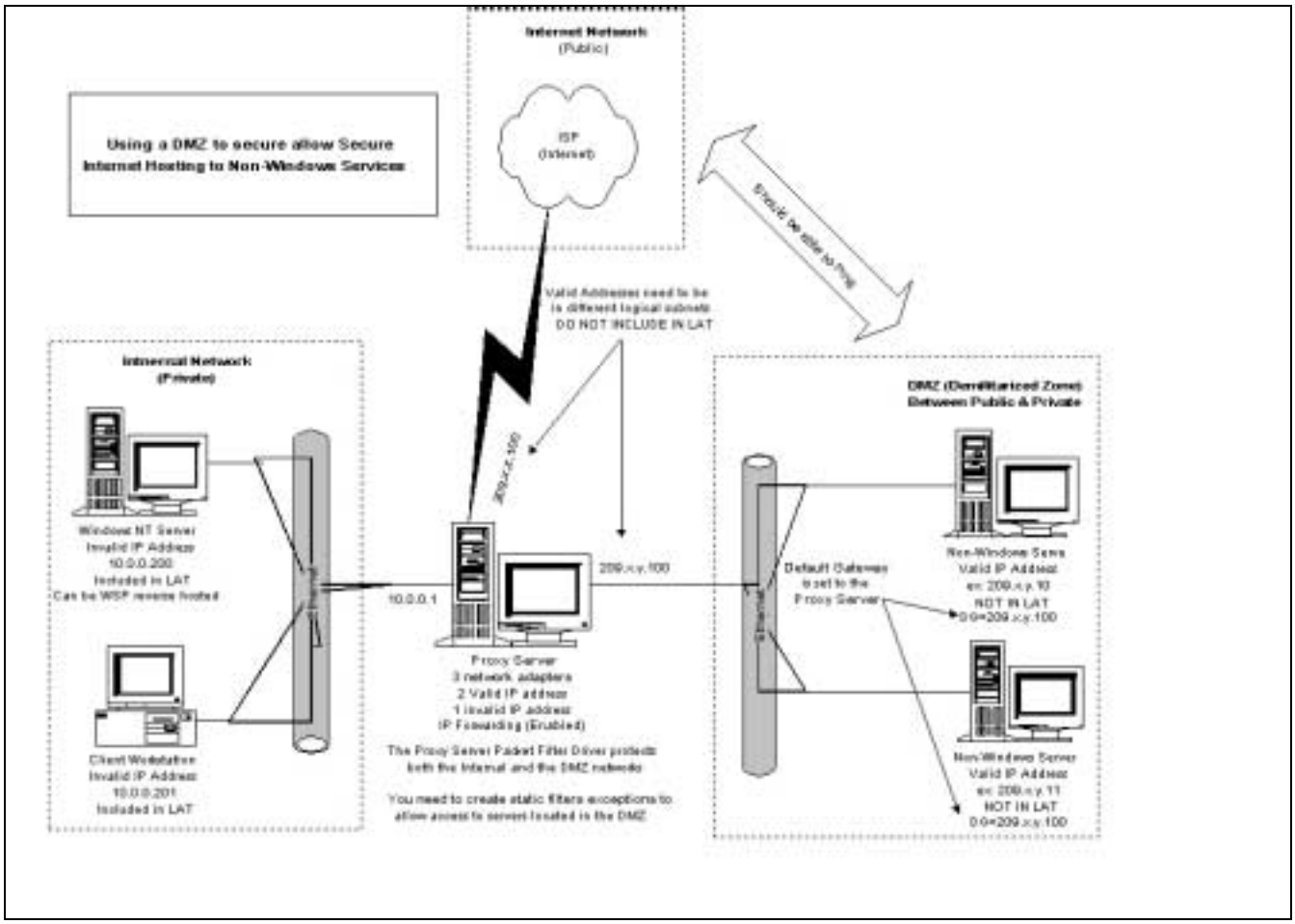
Nous avons déjà vu (paragraphe 4.3) que mettre en place une DMZ est la seule solution envisageable lorsque sont utilisées des applications qui ne sont pas gérées par les services du serveur Microsoft Proxy (ni HTTP, ni Winsock, ni SOCKS). Il en est de même lorsqu'il est nécessaire de publier sur Internet des serveurs non gérés par le serveur Proxy mais qui doivent être tout de même protégés par ce dernier.

Une DMZ est généralement utilisée avec Microsoft Proxy Serveur lorsque les fonctions proxy serveur et proxy inverse (voir paragraphe 11.3.) ne peuvent être utilisées. Si vous utilisez un système d'exploitation Apple, UNIX, OS/2 ou autre et que vous ne publiez pas sous HTTP, la configuration d'un réseau DMZ est obligatoire.

La fiche Q191146 détaille la mise en place d'une telle zone. En nommant A le réseau Internet, B la DMZ et C l'intranet, il est possible de résumer les étapes de la manière suivante:
- **installer un serveur Proxy avec trois cartes (respectivement A, B et C).** Les cartes A et B doivent disposer d'adresses Internet valides (ainsi que toutes les machines sur la DMZ). De plus les réseaux A et B doivent être dans des sous réseaux logiques IP différents.
- **incluez dans la LAT les adresses de machines Intranet ET celle de la carte B MAIS pas les machines de la DMZ.** Les machines de la DMZ ne sont pas

considérées comme faisant partie du réseau privé: le Trafic entrant et sortant de ces machines passent par le routage IP et non par des services du serveur Proxy (notre hypothèse dit effectivement qu'il ne les supporte pas)

- **Activez le routage IP sur l'ordinateur Proxy Serveur.** Ceci pour s'assurer que les machines clientes de l'Internet peuvent accéder aux serveurs de la DMZ. Pour cela il faut que le routeur qui relie le réseau A à Internet soit spécifie le serveur Proxy comme passerelle par défaut, soit qu'une route statique pour atteindre le réseau B soit spécifié comme devant passer par la carte A.
- **de même, les machines de la DMZ doivent pouvoir répondre sur le Web et donc doivent avoir une passerelle par défaut qui est la carte B.**
- **l'activation du routage IP a laisser des trous de sécurité dans votre serveur Proxy, il faut donc activer le filtrage de paquet et ne laisser passer que ce qui est nécessaire à direction des machines de la DMZ.** C'est ce filtrage qui permet à Proxy de sécuriser l'accès aux machines de la DMZ. Dans ce cas Proxy Serveur agit comme FireWall et non plus comme Proxy.



11.3. Le "Reverse Proxying"

a) Considérations générales

Nous avons vu comment configurer une application Winsock pour écouter sur la carte externe d'un serveur Proxy (voir paragraphe 7.5).
Nous allons voir maintenant comment faire pour qu'un serveur Winsock (Exchange, SQL, ...) puisse faire de même, c'est à dire que le serveur Proxy écoute pour le compte de ce serveur sur sa carte externe et transmette le trafic entrant et sortant au client.
En se basant sur le fait qu'un serveur qu'un serveur Winsock n'est rien d'autre qu'un exécutable Winsock, il apparaît que la méthode est strictement identique a celle employée avec une application cliente et tout ce qui a été vu dans le paragraphe 7.5 reste valable.
C'est dans ce cas par contre que le paramètre ProxyBindIp prend toute sa valeur, il permet à un serveur Proxy d'écouter pour le compte de plusieurs serveurs et si l'adresse IP est déjà utilisée sur la carte externe (par le serveur lui-même pour un service local ou par un autre serveur intranet qui déporte son service sur le Proxy) de spécifier une autre adresse.

Mis à part le cas d'Exchange détaillé dans le paragraphe ci-après, la fiche technique Q177153 détaille bien ce type de configuration pour des serveurs SQL, cc:Mail et Lotus Notes.

b) Un exemple détaillé et classique: Exchange

Exchange et son service SMTP, du fait de son lien avec l'Internet et le meilleur exemple de service qui gagne à être déporté sur la carte externe du serveur Proxy.
Cela permet d'envoyer et de recevoir des mails depuis l'Internet sur le serveur Exchange privé sans exposer le serveur lui-même à l'Internet.

Les fiches techniques qui traitent de ce sujet sont nombreuses:
- Q178532: Configuring Exchange Internet Protocols with Proxy Server
- Q181420: How to Configure Exchange or Other SMTP with Proxy Server
- Q181847: How to Configure Exchange Server with Proxy Server
- Q187650: Error: "Server Returned Invalid or Unrecognized Response"
- Q198509: "Unable to get your inbox" Using OWA via Proxy Server
- Q207655: Setting Up Web Publishing and OWA Access Through a Proxy

En résumé, la procédure classique (et qui suffit dans bien des cas) se résume en les étapes suivantes:

1. Installer sur le serveur Exchange le client WSP et le configurer pour utiliser le serveur Proxy approprié.

2. Configurer le serveur Exchange pour utiliser comme serveurs DNS des serveurs qui se trouvent sur l'Internet (ceux de l'ISP par exemple)

3. Vérifier que le client WSP marche bien (faire un FTP depuis la ligne de commande sur un serveur FTP Internet par exemple)

4. Modifier (ou faire modifier à l'ISP) l'enregistrement qui décrit votre serveur de mail (MX) pour être toujours le nom de votre serveur Exchange mais en étant associé maintenant à l'adresse de la carte externe de votre serveur Proxy.

5. Créer deux fichiers WSPCFG.INI avec Notepad. L'un d'eux servira pour l'IMC (Internet Mail Connector) et l'autre pour le Store d'Exchange.
   Je vous conseille TRES fortement de copier/coller les lignes de code pour ces fichiers depuis la base de connaissance (et surtout pas depuis ce document Word), article Q181420, ET DE NE PAS CREER LES FICHIERS A PARTIR D'UN DOCUMENT NOTEPAD VIDE.

6. Placer le premier fichier WSPCFG.INI (vérifiez l'extension) contenant le code suivant

   ```
   [MSEXCIMC]
   ServerBindTcpPorts=25
   Persistent=1
   KillOldSession=1
   ```

   dans le répertoire de l'exécutable de l'IMC:

   C:\EXCHSRVR\CONNECT\MSEXCIMC\BIN\WSPCFG.INI

   (ceci est répertoire par défaut, il est possible que ce dernier ne soit pas adapté si les répertoires par défaut d'Exchange ont été modifiés à l'installation)

7. Placer le deuxième fichier WSPCFG.INI (vérifiez l'extension) contenant le code suivant

   ```
   [STORE]
   ServerBindTcpPorts=110,119,143
   Persistent=1
   KillOldSession=1
   ```

   dans le répertoire de l'exécutable du store:

   C:\EXCHSRVR\BIN\WSPCFG.INI

   (même remarque que précédemment)

8. Donner au compte de service Exchange les droits illimités au niveau du service Winsock Proxy (vous pourrez toujours définir au mieux les permissions après comme utiliser CREDTOOL si vous le voulez...mais dans un deuxième temps)

9. Retirer tout filtrage de paquet sur le serveur Proxy (à (re)mettre éventuellement après... dans un deuxième temps)

10. Redémarrer le serveur Exchange et le serveur Proxy

11. Procéder à des tests: en utilisant NETSTAT pour voir les ports sur lesquels écoute le serveur Proxy côté Internet et envoyer des mails depuis TELNET

```
"
 helo <serveur exchange>.<domaine>.<organisation>
 mail from <un utilisateur bidon>@<un domaine bidon>.<organisation>
 rcpt to: <une boite aux lettre existante>@<domaine>.<organisation>
 data
 Ceci est un test.
 .
 quit
"
```

12. Administrer son serveur

12.1. Le Microsoft® Proxy Server Web Administration Tool

Il permet d'administrer un serveur Proxy depuis un browser.
Cet outil qui se greffe sur l'IIS sur lequel s'appuie le serveur Proxy, et est disponible en téléchargement depuis l'adresse suivante :
http://www.microsoft.com/proxy/downloads/proxyadmin.asp

12.2. Arrêter et redémarrer les services

Les services Winsock, Socks et Web Proxy sont exécutés avec le service Web d'IIS. Pour arrêter ou démarrer l'un ou l'autre service vous devrez arrêter le service W3SVC :

```
NET STOP | START W3SVC
```

12.3. Les logs Proxy sur ODBC

Pour toute machine ne disposant pas du SP1 (donc toutes les machines en IIS3 entre autre), il existe une série de correctifs à mettre en place pour assurer la journalisation via ODBC.

Le plan d'action suivant est à mettre en œuvre :

- **Sur le serveur SQL :**

En suivant les instructions des articles Q177707 et Q218435, s'assurer des tables SQL.

- **Sur le serveur Proxy :**

1- Appliquer le proxy combined hotfix (Q190997, correctif en Français disponible). Ne pas redémarrer la machine.
2- réappliquer le SP4. (redémarrage de la machine)
3- Vérifier bien que la valeur LogType soit à "2" sous HKEY_LOCAL_MACHINE\system\CurrentContolSet\Services\W3Proxy\Parameters

5- Appliquer les correctifs Q19644 et Q196445 (ces correctifs n'existent qu'en version US mais ils ont été testés avec succès sur des machines françaises)

6- redémarrer le serveur Proxy et procéder a un test.

12.4. Les compteurs de performance

Avec l'installation de Proxy serveur sont installés les compteurs Perfmon suivants:
- Web Proxy Server service
- Web Proxy Cache
- WinSock Proxy service
- Socks Proxy service
- Packet filter

Les compteurs les plus couramment utilisés sont inclus dans les deux premiers objets:

Web Proxy Server service:
- Sites denied: si ce compteur est important, peut être avez-vous bloqué des sites qui ne devraient pas l'être.
- Current users: permet de suivre le nombre de personnes utilisant le serveur. Utile également quand un redémarrage du serveur est à envisager.
- Maximum users: le nombre maximum d'utilisateurs qu'il y a eu à un instant t.
- Inet bytes total/sec: nombre total d'octets échangés entre le serveur et Internet , cela permet de savoir si le serveur utilise peu ou trop la bande passant disponible avec le fournisseur d'accès Internet.

Web Proxy Cache:
- Bytes in cache: a comparer avec la taille du cache configuré dans le serveur, si on est proche de cette limite, il faut penser à augmenter la taille du cache.
- Active refresh bytes rate : pour déterminer s'il est nécessaire d'augmenter ou diminuer le cache actif.

Avec l'installation de Proxy est également créé un jeu de compteurs prédéfinis (Msp.pmc) avec un icône dans le menu Démarrer, il contient:

% Processor Time: Ce compteur affiche le temps processeur consommé par les processus InetInfo ET WSPSRV. Si cette valeur est trop élevée (70-80% en moyenne) il faut d'abord s'assurer que cette valeur n'est pas due a un processus bloqué et dans un deuxième temps, augmenter les capacités de la ressource processeur (soit en nombre soit en vitesse)

Cache Hit Ratio(%): montre a quel point le cache est utile et bien configuré par rapport aux besoins des utilisateurs.

12.5. Utilisation des alertes

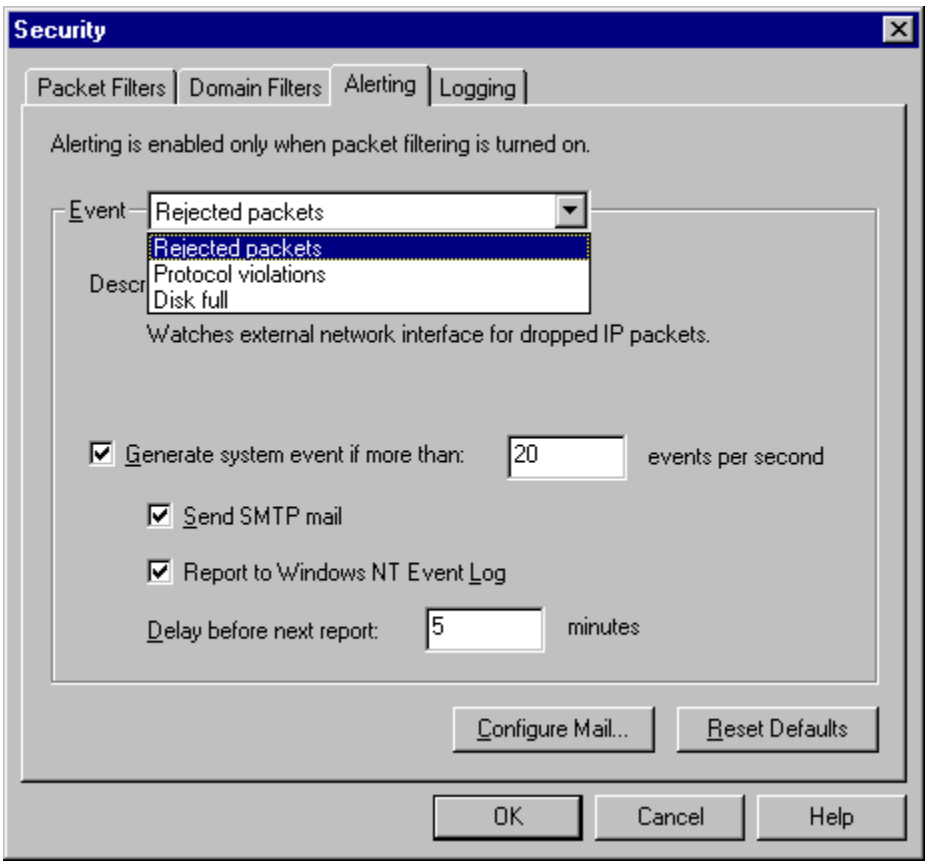
Vous pouvez contrôler votre réseau et émettre des alertes lorsque des événements douteux surviennent sur le réseau comme les paquets rejetés ou les violations de protocole ou lorsqu'un disque de Proxy Serveur est plein.
Les événements sont enregistrés dans le journal de filtrage de paquets et dans les journaux des services de Proxy Serveur. Ils peuvent aussi être enregistrés dans le journal d'événements de Windows NT ou envoyés sous forme de message électronique au destinataire que vous avez spécifié. De plus, Proxy Serveur peut générer des rapports concernant les paquets pour signaler qu'aucun service système n'était à l'écoute. Il est recommandé de revoir les journaux afin de déterminer l'origine des événements.

L'événement paquets rejetés est généré lorsque de nombreux paquets sont perdus ou lorsqu'il existe des erreurs dans les trames. Par exemple, si le taux de perte des paquets est élevé pendant une période donnée, votre réseau subit probablement une attaque. Vous pouvez spécifier la fréquence de paquets rejetés au-delà de laquelle Proxy Serveur doit générer un événement.

L'événement violation de protocole est généré lorsque les paquets ou trames filtrés ne respectent pas la structure de protocole autorisée. Votre réseau subit probablement une attaque.

L'événement disque plein est généré lorsque le disque sur lequel est enregistré l'un des journaux de service ou le journal des paquets est plein.

Remarque Vous devez d'abord activer le filtrage de paquets pour que les alertes en cas d'événements paquets rejetés et violation de protocole soient activées.



12.6. Le futur: Hit List Proxy Analyzer (HLPA)

Microsoft prépare la sortie d'un analyseur de journal Proxy générant des rapports (un peu similaire à ce que fait usage analyst de Site Server).
Cet outil est gratuit et fonctionne sur Windows 9x et NT 4.0.
(il est disponible en interne \\Comet\Public\Nevet\hl40mp.exe)

Les différentes fonctionnalités de ce logiciel sont:

- Comprendre les habitudes de browsing des utilisateurs de manière à prévoir les évolutions de la charge et de l'utilisation de la bande passante.
- Détecter les abus du Web et sa "mauvaise" utilisation.
- Mesurer l'activité Intranet
- Mesurer l'efficacité du cache et de son paramétrage
- Mesurer la productivité des utilisateurs

13. Conclusion

Microsoft Proxy Serveur a de multiples utilisations et son intégration dans des environnements complexe doit commencer par une étude de l'existant et des modifications qu'elle va entraîner.

Pour d'autres informations, je conseille les documents suivants:

- "Tips from the Proxy Gurus, Configuring & Trouble-Shooting Services and Applications to work with
MS Proxy 2.0 FAQ", de Jeff Wierer et Daniel Mosmeyer

- "Microsoft Proxy Server Security and Evaluation" de Coopers & Lybrand L.L.P. Information Technology Security Services

- "Cache Array Routing Protocol and Microsoft Proxy Server 2.0", White Paper Microsoft

Et, bien sûr, le lien officiel: http://www.microsoft.com/proxy/default.asp