

# Présentation générale d'ISA Server 2004

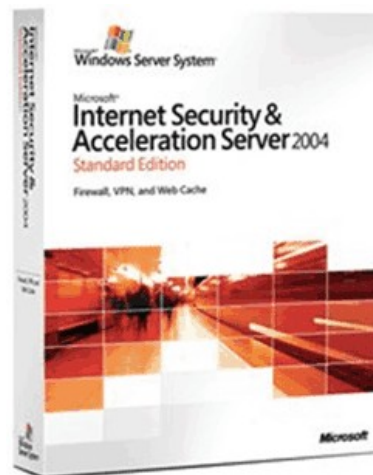
## Introduction

La sortie d'**Internet Security & Acceleration Server 2004** durant le mois de Juillet (2004) a été un évènement très important pour Microsoft. En effet ce logiciel apparaît comme étant **l'élément clef de la politique de sécurité** actuellement instaurée par la firme en question.

Pour rappel, cette politique est essentiellement composée de quatre points :

- Une **augmentation du niveau de sécurité par défaut** pour les applications (on peut par exemple citer le firewall de Windows XP qui s'active automatiquement dès l'installation du Service Pack 2).
- Une **maintenance et un déploiement facilité des mises à jour** grâce à de nouveaux outils (SUS, MBSA, SMS, WSUS ...).
- Un **meilleur niveau de sécurité** dans le développement (Microsoft assure que le code de ses prochaines applications sera plus « sécurisé »).
- Une meilleure **sensibilisation des utilisateurs** et notamment du grand public sur le problème de la sécurité via un site web dédié.

Après un tel discours et étant donné le contexte actuel (spam, vers et virus sont devenus le quotidien des internautes et le cauchemar des administrateurs), Microsoft se devait de lancer une mise à jour convaincante de son logiciel phare concernant la sécurité.



---

## Acronymes :

MBSA : Microsoft Baseline Security Analyzer (Logiciel permettant d'analyser le système d'exploitation)

SUS: Software Update Services

WSUS: Windows Server Update Services

NAT : Network Address Translation

IIS : Internet Information Services

VPN : Virtual Private Network

SMTP : Simple Mail Transfer Protocol

SNMP : Simple Network Management Protocol

RDP : Remote Desktop Protocol (Microsoft Terminal Services)

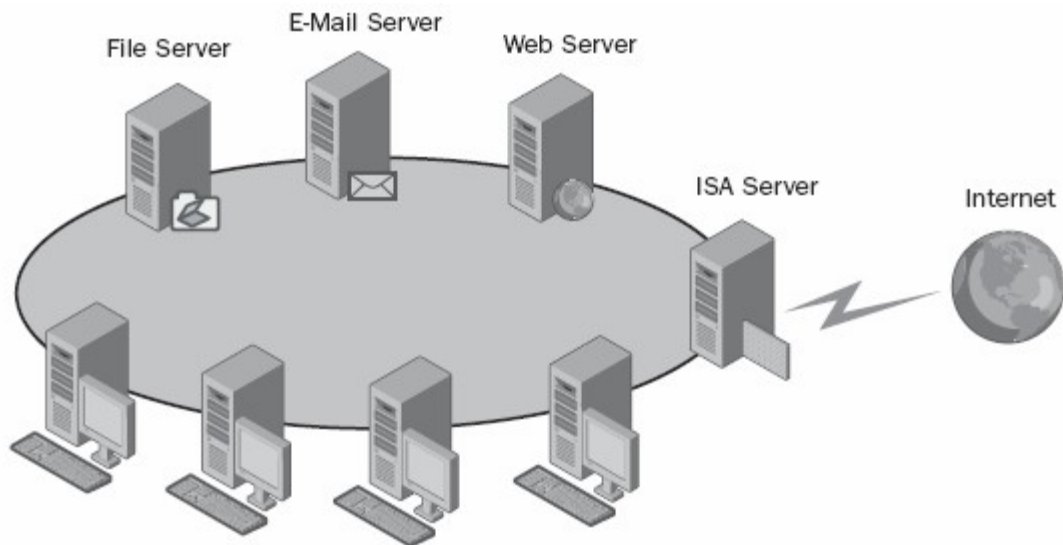
LDAP : Lightweight Directory Access Protocol (permettant l'interrogation des services d'annuaire)

FQDN: fully qualified domain name

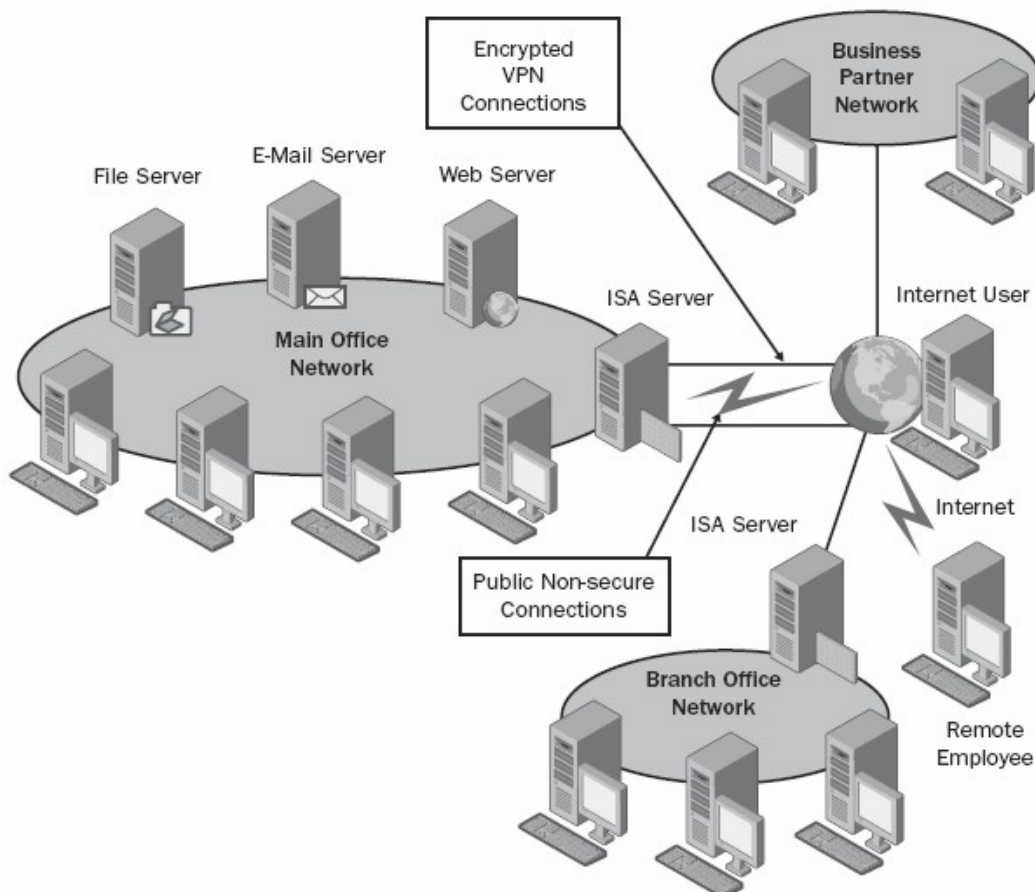
MAC :(Media Access Control address)

Hyperthreading : consiste à créer deux processeurs logiques sur une seule puce, chacun doté de ses propres registres de données et de contrôle.

Le serveur ISA 2004 est conçu pour sécuriser le périmètre du réseau d'une organisation. Dans la plupart des cas, ce périmètre se situe entre le réseau local interne de l'organisation (LAN) et un réseau public tel que l'Internet. Le schéma suivant montre un exemple de déploiement d'un serveur ISA 2004 :



Malheureusement ce schéma montre un exemple simple d'une configuration réseau où la frontière entre le réseau interne d'une organisation et l'Internet est facile à définir. En réalité, la définition de la frontière entre le réseau interne d'une organisation et le reste du monde n'est pas aussi simple. Le schéma qui va suivre montre un cas plus compliqué, mais plus réaliste.



Il est beaucoup plus difficile définir le périmètre d'un réseau dans un scénario tel que celui représenté sur le schéma précédent. Par exemple, les exigences de compagnie peuvent signifier que la frontière entre le réseau interne et l'Internet peut être croisée de plusieurs manières différentes :

- N'importe quel utilisateur d'Internet devrait pouvoir accéder au site Web public.
- Les utilisateurs d'une organisation d'associés devraient pouvoir accéder au site Web privé avec certaines limitations d'accès.
- Les utilisateurs d'une succursale devraient avoir accès complet aux ressources du réseau interne. Le seul raccordement entre la succursale et le réseau interne principal est l'Internet.
- Les employés de qui sont hors du bureau et qui dispose d'une connexion Internet devraient avoir accès aux ressources de réseau interne, y compris l'email et les serveurs d'archivage.
- Les utilisateurs du réseau interne devraient pouvoir accéder à Internet avec des applications spécifiques et à un nombre limité de ressources sur le réseau externe.

## **1.2 Nouveautés par rapport à la version 2000**

Pour commencer, rappelons qu'ISA Server ne joue pas simplement le rôle de **pare-feu** mais aussi de **serveur de Proxy** et de **serveur VPN**. Voici une liste non exhaustive des principales nouveautés et améliorations apportées depuis la version 2000 :

- Une **nouvelle interface graphique** beaucoup plus ergonomique et intuitive.
- Le paramétrage des règles de routage/NAT entre les différents réseaux connectés au serveur ISA a été révolutionné grâce à la création d'un **assistant de configuration réseau** qui permet de se décharger totalement de cette opération et permet ainsi de se concentrer sur le paramétrage des options liées à la sécurité.
- La **configuration des règles du pare-feu a été entièrement revue** par rapport à la version 2000 notamment au niveau de l'ordre d'application des règles.
- De **nouveaux filtres applicatifs** ont été ajoutés ou modifiés. Par exemple le filtre HTTP a été grandement remanié afin d'augmenter le niveau de sécurité des applications web comme IIS, Exchange ou bien encore Outlook.
- Les **possibilités au niveau de la surveillance** (ou monitoring) ont été développées en profondeur. Ainsi on pourra visualiser les journaux (logs) et les sessions actives en temps réel, importer et exporter des rapports au format HTML, tester la connectivité réseau,...
- Le serveur VPN est dorénavant totalement intégré au serveur ISA et son paramétrage en est d'autant plus facilité.
- La possibilité d'**importer et d'exporter la configuration du serveur ISA au format XML**.
- Si vous souhaitez prendre connaissance de l'ensemble de modifications et des nouveautés par cette nouvelle version, deux alternatives s'offrent à vous :

## **1.3 Configuration requise**

Voici les caractéristiques logicielles et matérielles requises pour exécuter ISA Server 2004 :

- processeur **Pentium III 550** ou plus performant
- **256Mo** de mémoire vive
- un nombre de cartes réseaux et/ou modems adéquats
- une partition ou un volume formaté avec le **système de fichier NTFS** et disposant de **150Mo d'espace libre** (bien entendu, si vous souhaitez activer la mise en cache, il faudra disposer de plus d'espace).
- un minimum de deux interfaces réseau (carte réseau, modem ADSL,...)
- **Windows Server 2003 ou Windows 2000 Server SP4**

- **Internet Explorer 6.0** ou supérieur

Bien entendu vous devrez tenir compte du nombre de clients connectés "derrière" le serveur ISA ainsi que des fonctions que vous activerez pour ajuster le matériel de votre serveur.

#### **1.4 Les différentes versions disponibles :**

La version Standard ne peut gérer qu'un maximum de 4 processeurs physiques.

En ce qui concerne la restriction appliquée au niveau du nombre de processeur, elle prend uniquement en compte **les processeurs physiques**. Ainsi il est possible d'utiliser l'édition standard du serveur ISA sur un système équipé de 4 processeurs bi-cores supportant l'hyperthreading. Le système d'exploitation reconnaîtra seize processeurs mais seulement 4 processeurs seront comptés en ce qui concerne le licensing . Il est important de le préciser car tous les éditeurs de logiciels ne mènent pas la même politique vis-à-vis des processeurs supportant l'hyperthreading et/ou le multi-cores.

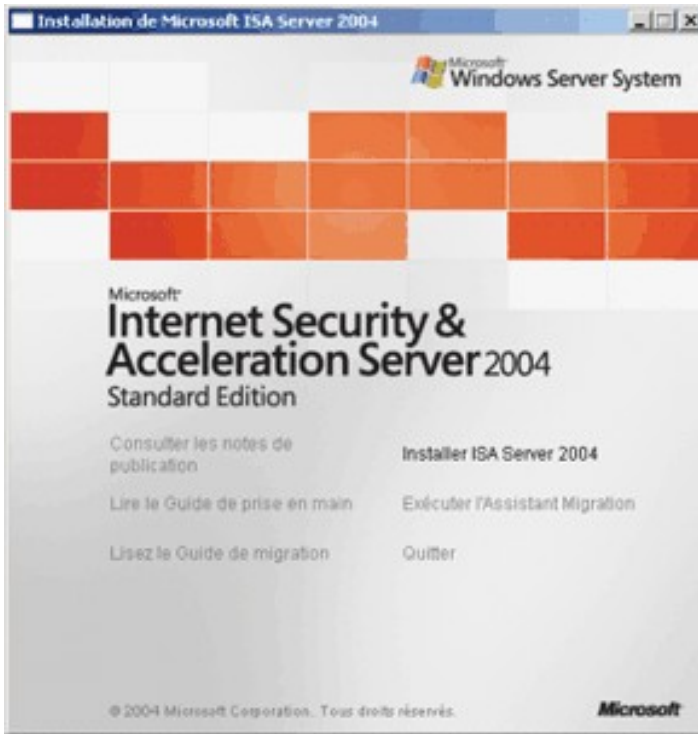
La version standard d'ISA Server 2004 ne comporta **aucune restriction en ce qui concerne la mémoire vive**. Les seules limitations à ce niveau seront celles du matériel et de l'OS (4Go sur la version standard de Windows Server 2003, 32Go sur la version Entreprise et jusqu'à 512Go sur la version 64 bits de Windows Server 2003 Datacenter Edition).

## **Installation et configuration initiale**

### **2.1 Installation du logiciel**

Contrairement à la version 2000 qui proposait 3 modes d'installation différents (mode cache, mode pare-feu et mode intégré), ISA Server 2004 ne propose qu'un seul mode d'installation. Dorénavant l'activation ou non de la mise en cache se paramètre dans la console de Gestion ISA et n'est plus tributaire du mode d'installation choisi au départ.

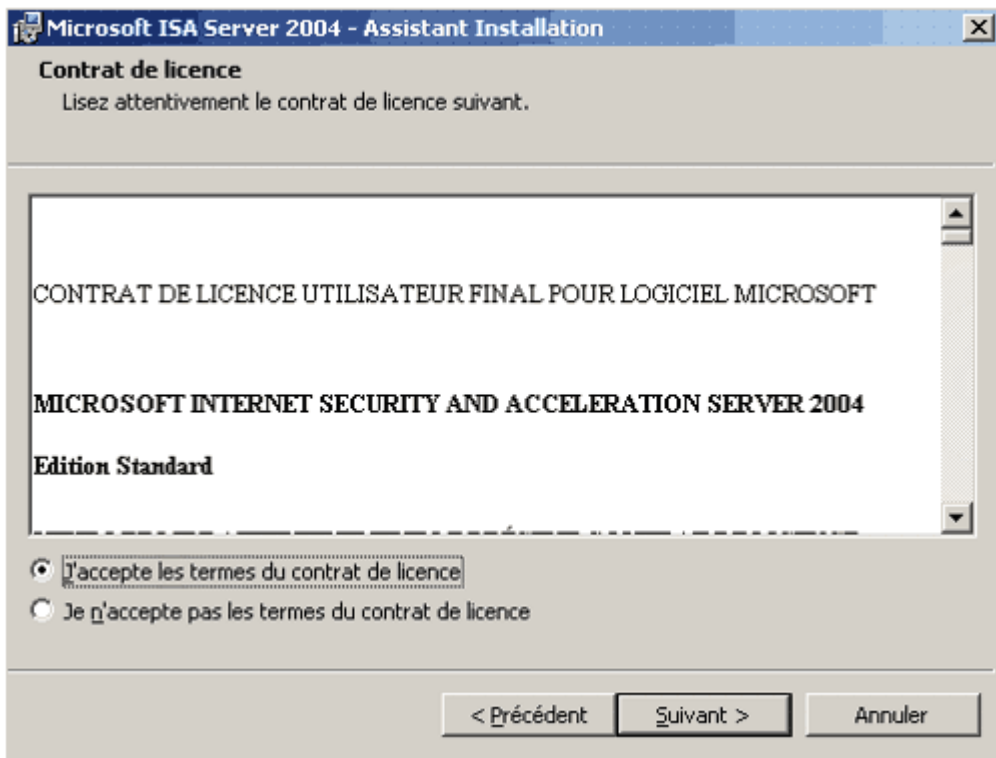
Après l'insertion du CD-ROM d'installation, le menu ci-dessous apparaît. Il permet d'installer ISA Server 2004 ou bien de mettre à jour un serveur exécutant ISA 2000. Pour réaliser une migration d'ISA 2000 vers ISA Server 2004, le Service Pack 1 pour ISA 2000 doit être installé au préalable.



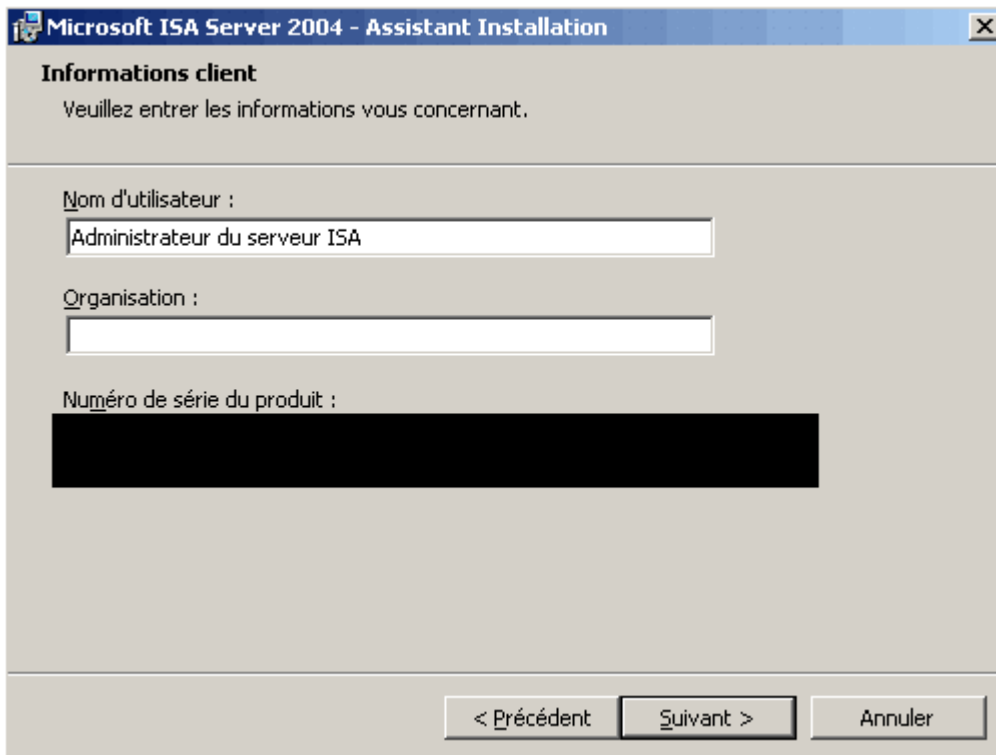
Une fenêtre vous invite à démarrer l'installation.



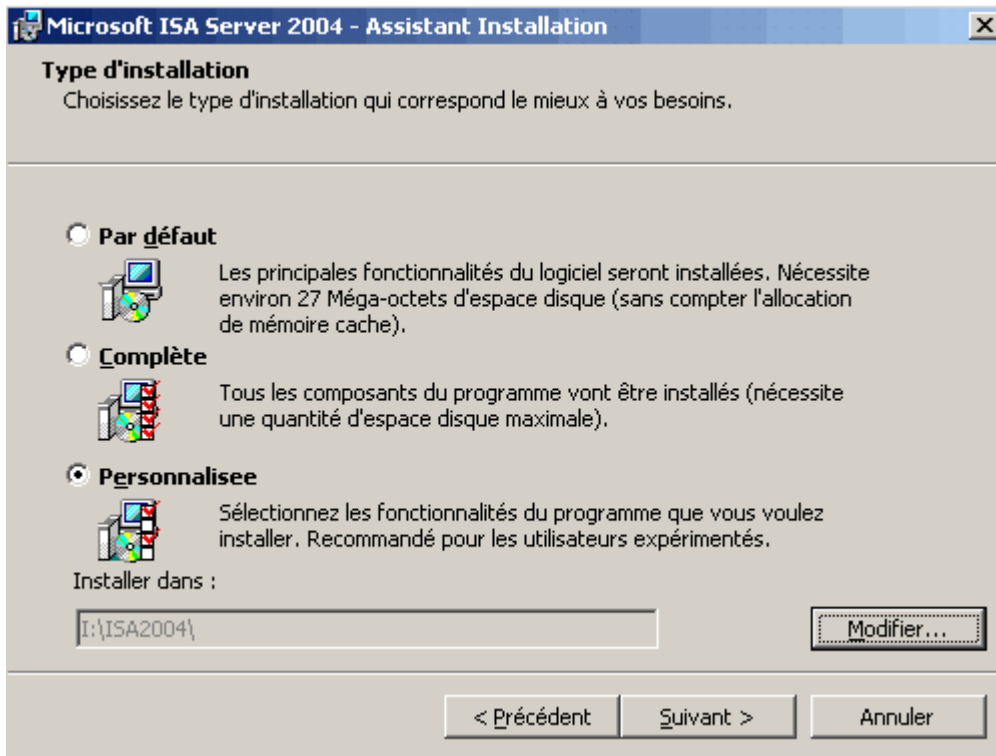
Le contrat de licence utilisateur rappelant les conditions d'utilisations légales du logiciel apparaît. Vous devez accepter les termes du contrat pour pouvoir poursuivre.



Vous devez ensuite rentrer un nom d'utilisateur, le nom de votre Société (optionnel) et le numéro de série du produit.

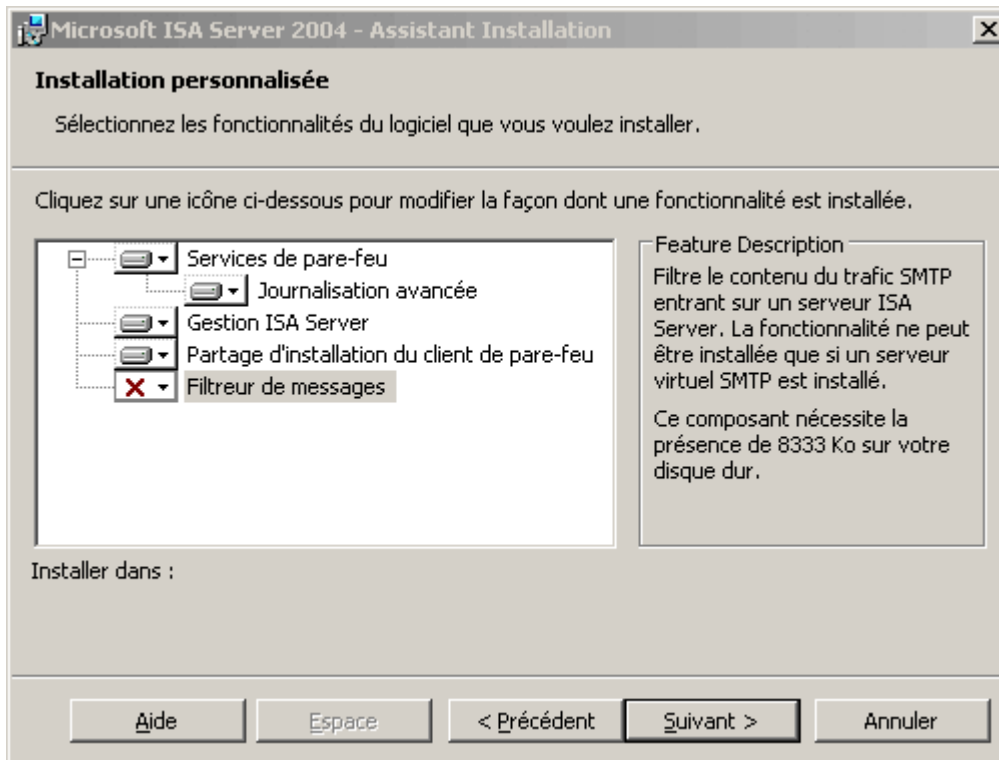


Vous devez ensuite sélectionner le type d'installation. Nous sélectionnons ici l'installation personnalisée afin de connaître toutes les options du programme.

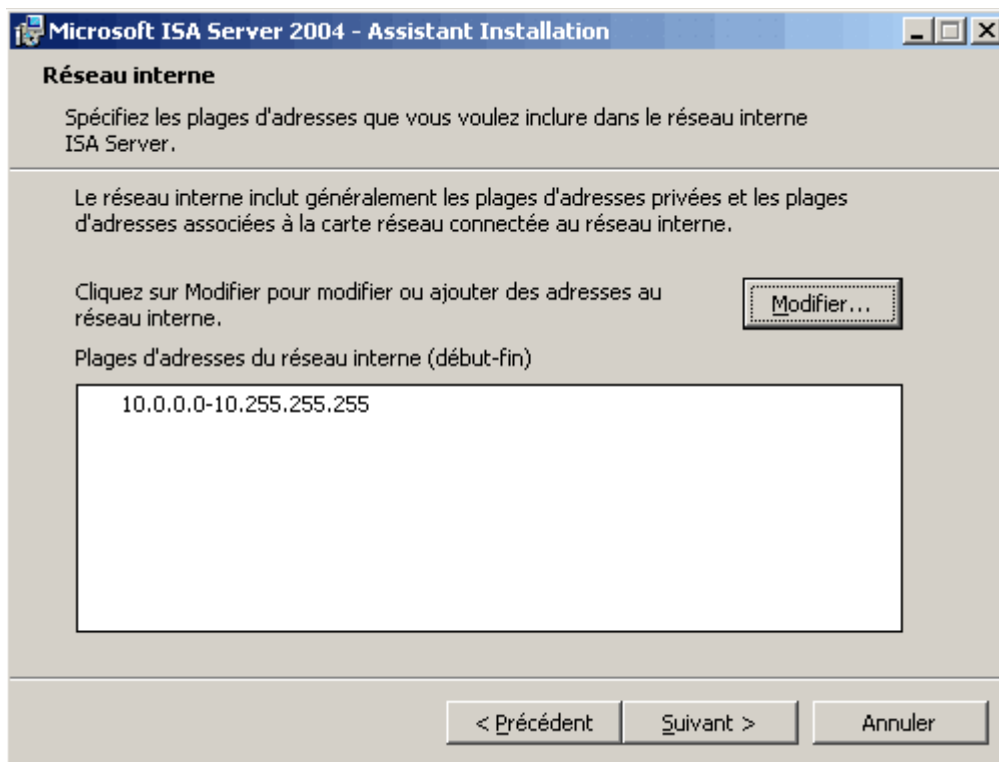


Les 4 principaux composants sont :

- o **services de pare-feu** : installe les services nécessaires pour filtrer les données transitant à travers le serveur ISA (indispensable sauf si on en souhaite utiliser le serveur ISA uniquement en tant que serveur de Proxy)
- o **gestion ISA Server** : installe la console de gestion qui permet de paramétrer le serveur ISA
- o **partage de l'installation du client pare-feu** : crée un partage réseau [\\nom de machine\mspclnt](#) qui contient les fichiers d'installation de la nouvelle version du client pare-feu (C:\Program Files\Microsoft ISA Server\Clients)
- o **filtreur de messages** : ce composant permet de filtrer le contenu du trafic SMTP entrant sur le serveur ISA.

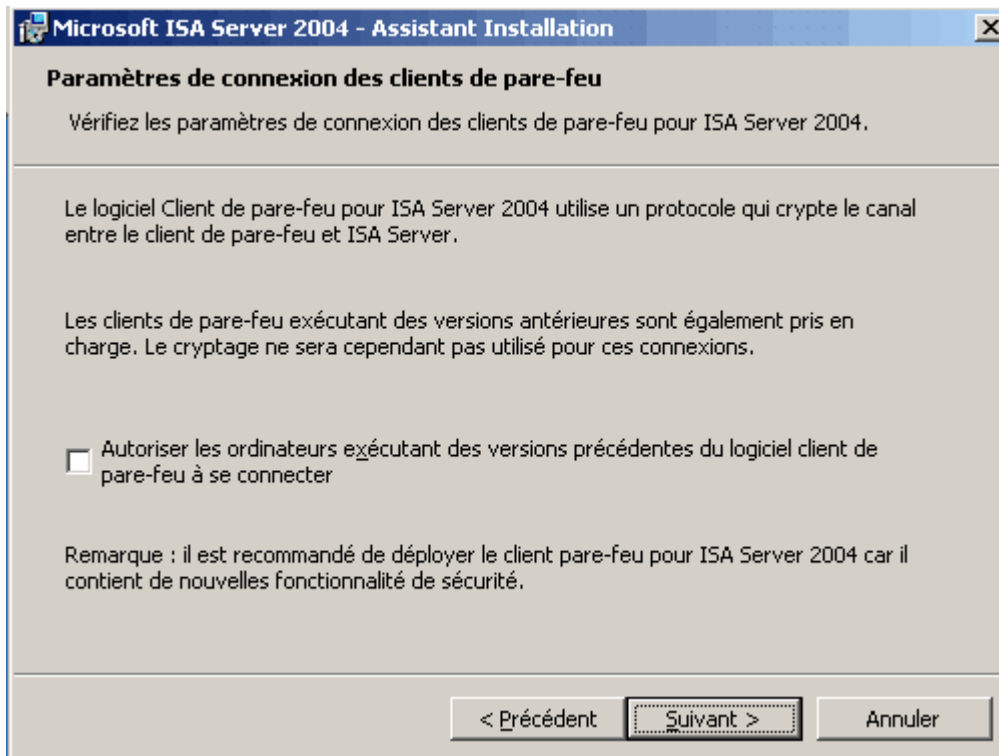


L'étape suivante est de saisir la table d'adresses locales, c'est-à-dire l'ensemble des plages d'adresses IP utilisées sur le réseau interne de l'entreprise.

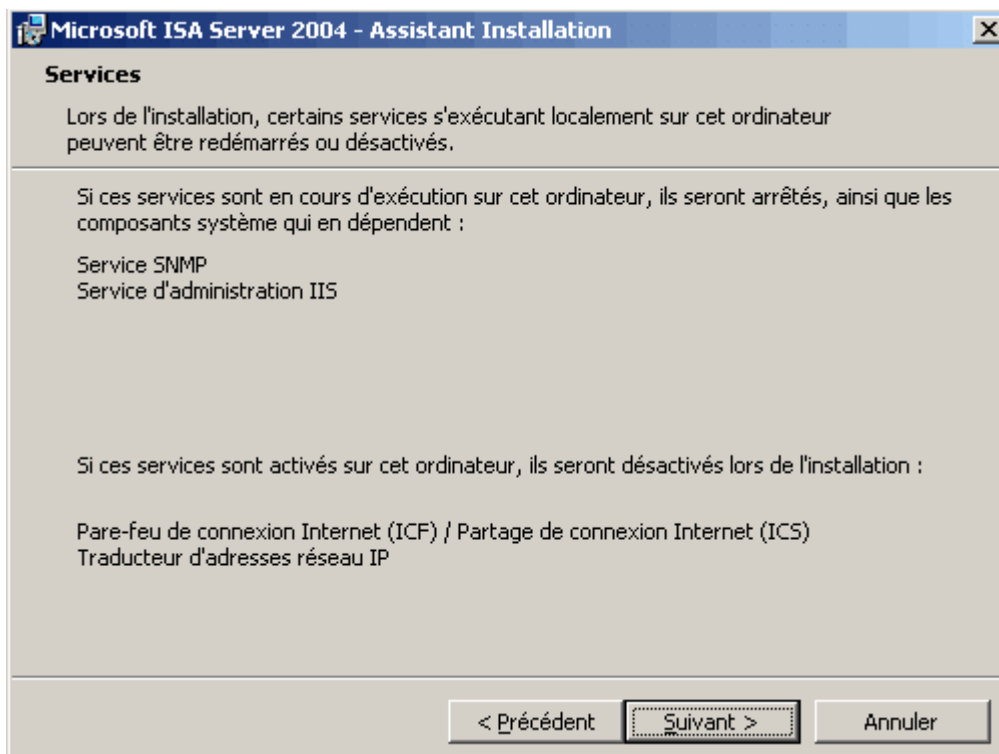


Il faut ensuite spécifier si les ordinateurs exécutant l'ancienne version du client pare-feu pourront se connecter au serveur ISA 2004. Par défaut les connexions des ordinateurs utilisant la version 2000 du client pare-feu se verront refusées.

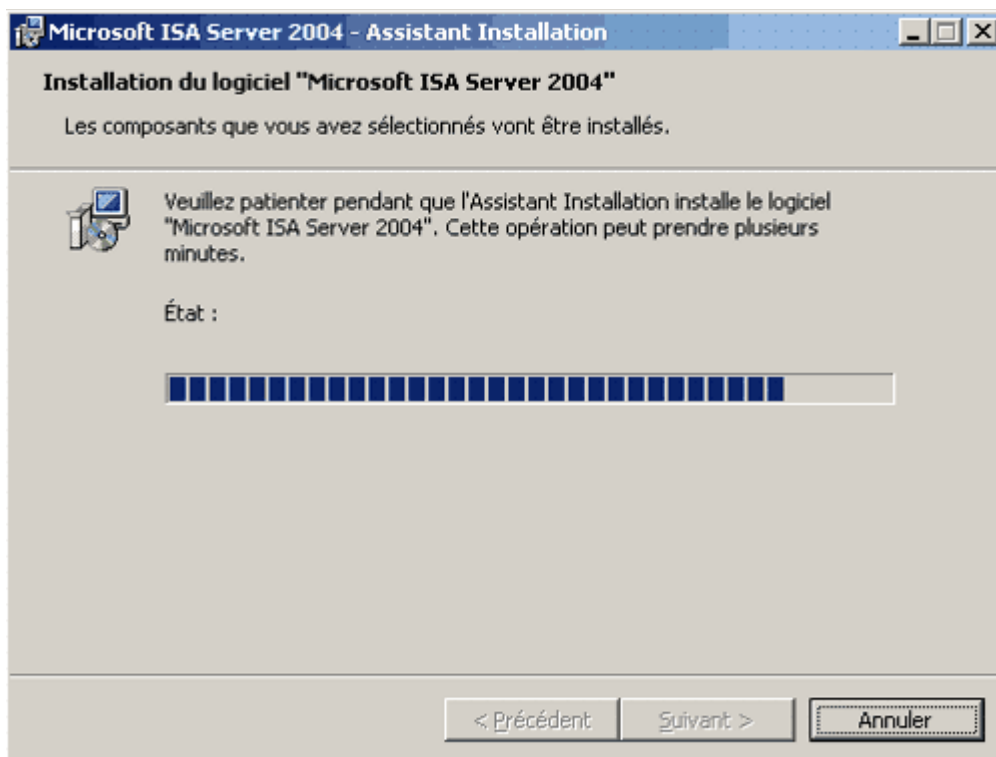
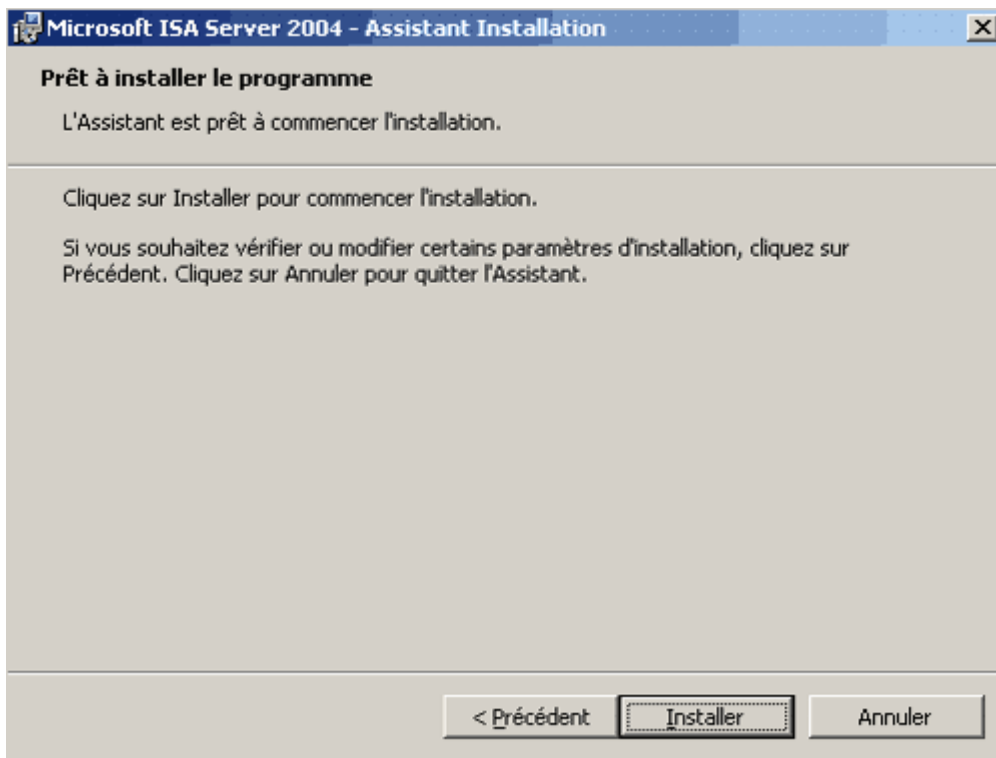




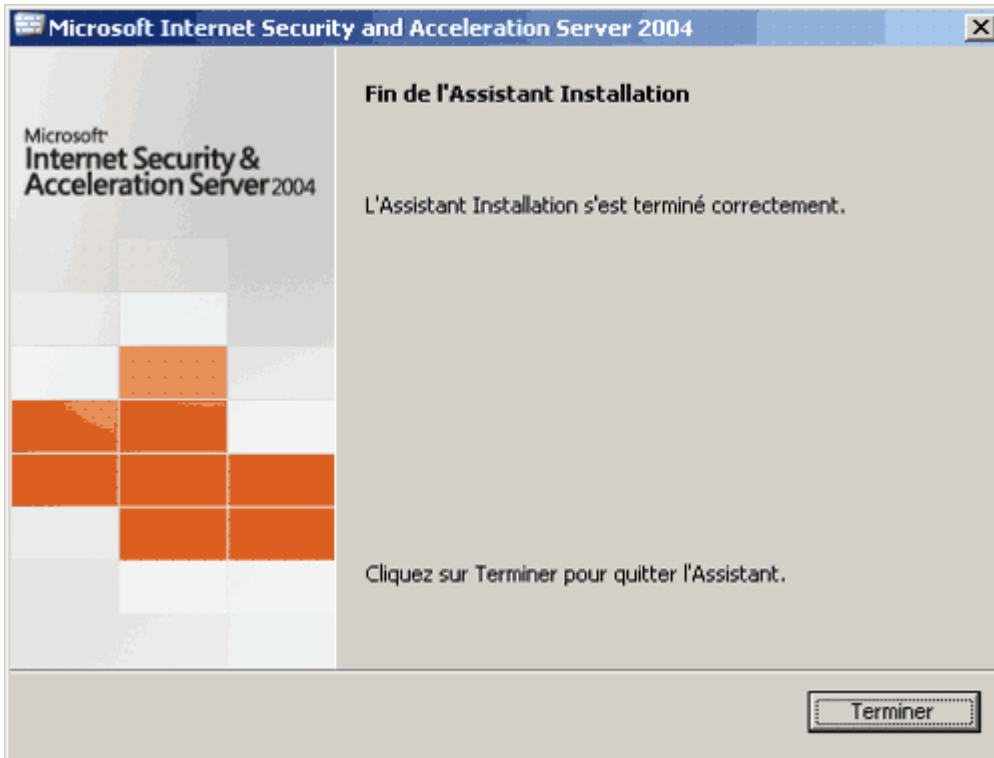
L'assistant d'installation averti que tous les services liés à des applications web vont être désactivés ou arrêtés durant l'installation.



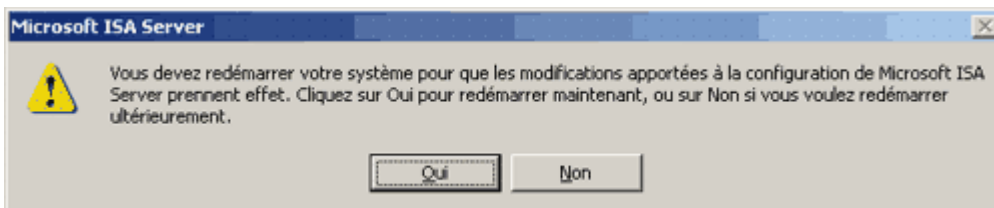
Tout est paramétré, il faut maintenant démarrer l'installation en cliquant sur suivant.



Une fenêtre vous avertis lorsque l'installation du programme est terminée.



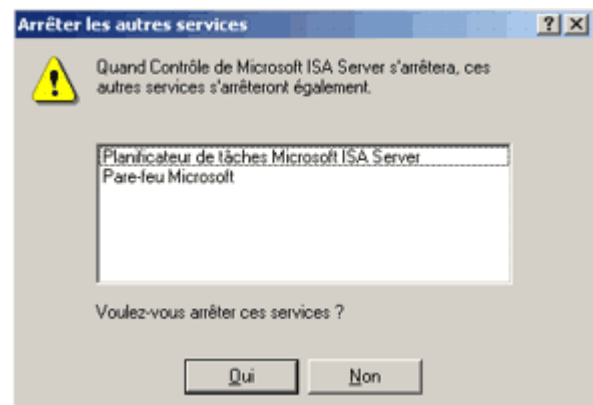
Vous êtes enfin invité à redémarrer le système d'exploitation.



Lors du démarrage, une page web sera automatiquement lancée et vous invitera à chercher d'éventuelles mises à jour pour ISA Server 2004. N'hésitez pas à réaliser cette opération. Une fois cela fait, il ne reste plus qu'à paramétrer le serveur grâce à la console dédiée à cette tâche.

Une fois l'installation terminée, six nouveaux services sont installés et doivent être démarrés pour que le serveur fonctionne correctement. Quatre de ces services concernent directement ISA Server :

- **Contrôle de Microsoft ISA Server** : ce service est le service principal d'ISA 2004. Il se révèle très utile pour arrêter/démarrer le service pare-feu et le service Planificateur de tâches Microsoft ISA Server en une seule opération.
- **Pare-feu Microsoft** : ce service est le plus important, il gère toutes les connexions faites au serveur, les règles du pare-feu, les règles de mise en cache, ... S'il n'est pas démarré, aucune des fonctionnalités du serveur n'est assurée (mise en cache, pare-feu et serveur



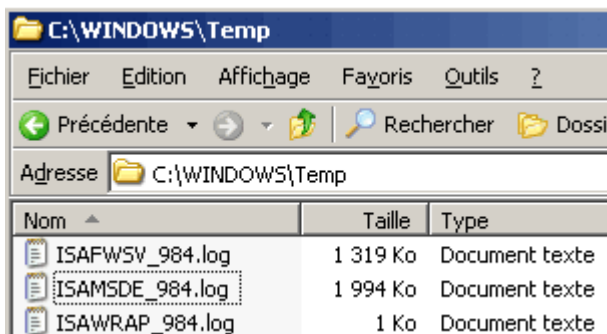
VPN).

- **Planificateur de tâches Microsoft ISA Server** : ce service permet de planifier des rapports sur l'activité du serveur.
- **Espace de stockage Microsoft ISA Server** : ce service gère notamment le système de surveillance intégré à ISA Server et l'espace mémoire nécessaire à la mise en cache .

Les deux autres services correspondent au moteur de SQL Server 2000. En effet, **MSDE 2000 version A** (pour Microsoft SQL Server Desktop Engine) est utilisé afin de stocker les données (notamment les données des journaux et des rapports) :

- **MSSQL\$MSFW**
- **MSSQLServerADHelper**

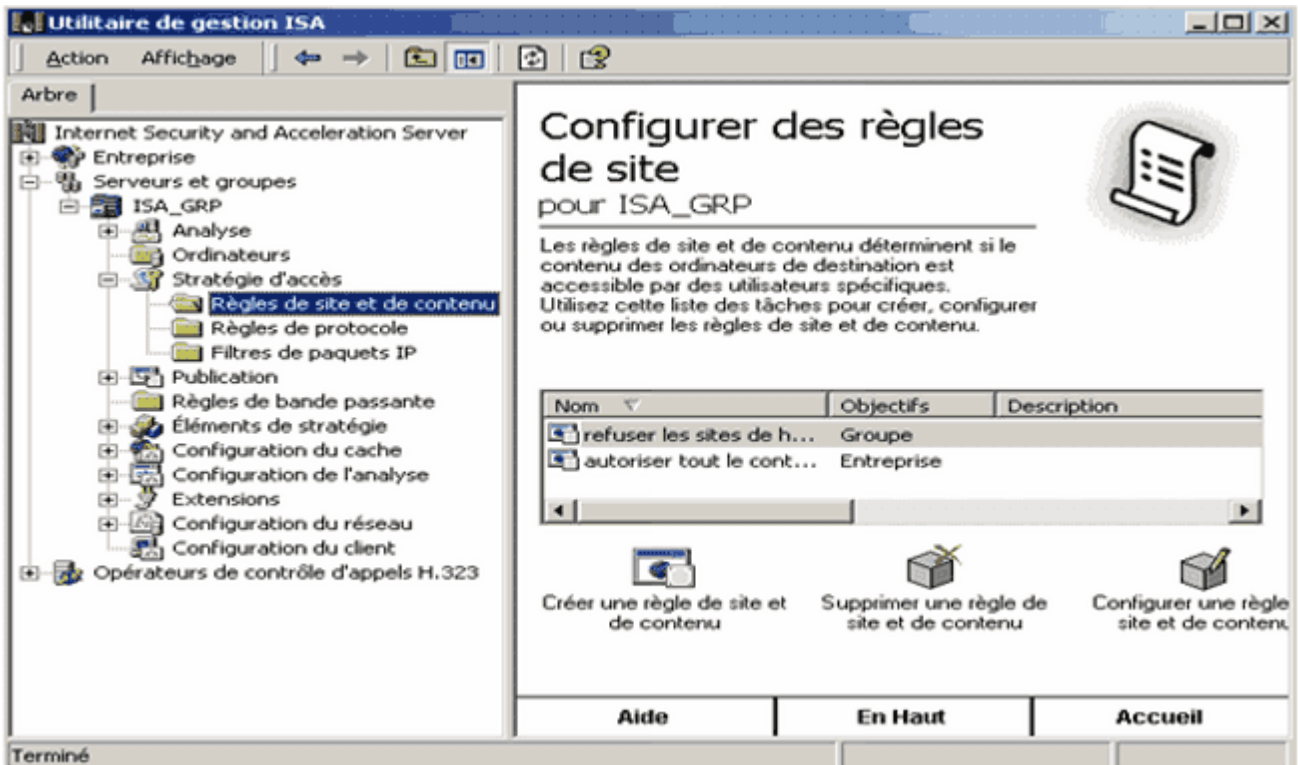
A l'issu du processus d'installation, il est conseillé de consulter les **trois fichiers journaux** générés dans le répertoire **%WINDIR%\temp**:



- le fichier **ISAWRAP\_xxx** contient un résumé du processus d'installation.
- le fichier **ISAMSDE\_xxx** contient des informations détaillées concernant l'installation du moteur de base de données MSDE.
- le fichier **ISAFWSV\_xxx** contient des informations détaillées concernant l'installation d'ISA Server.

## 2.2 Une interface entièrement repensée

Tout comme pour la version 2000, on utilise une console MMC (Microsoft Management Console) pour gérer le serveur ISA. Cependant, ISA Server 2004 a fait l'objet d'une **refonte totale au niveau graphique**. Outre le nouvel aspect bien plus esthétique grâce à ses formes arrondies, cette console « nouvelle génération » apporte **un réel plus en terme d'ergonomie** par rapport à l'ancienne console qui possède une lourde interface composée d'une arborescence compliquée et de menu mal conçus.

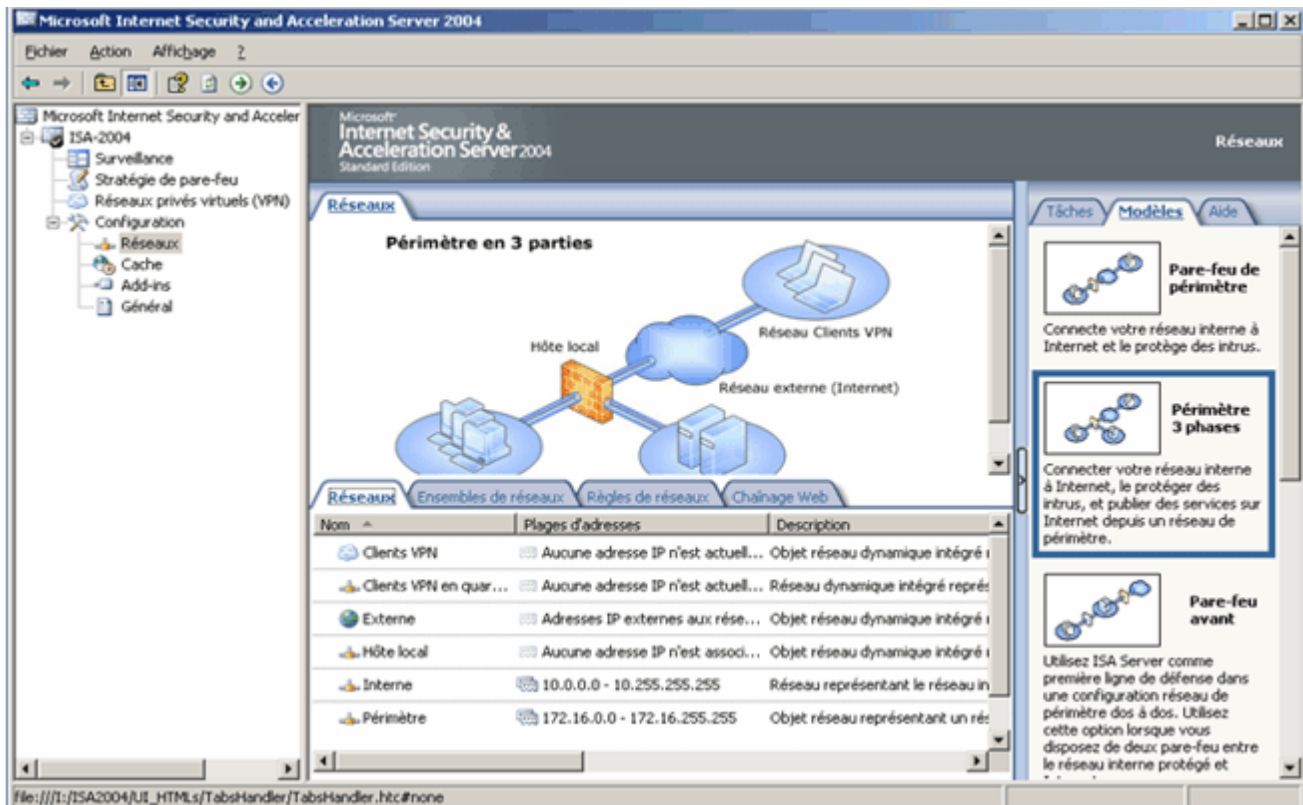


### La console de Gestion ISA version 2000

Comme vous pouvez vous en rendre compte le nouvel utilitaire de configuration conserve un système avec deux fenêtres. Cependant, la fenêtre de gauche présente dorénavant une arborescence bien plus simpliste composée de 4 menus principaux :

- **Surveillance**
- **Stratégie de pare-feu**
- **Réseaux privés virtuels (VPN)**
- **Configuration** (composée de 4 sous menus : Réseaux, Cache, Add-ins et Général)

Les autres options de configuration sont ensuite accessibles par le biais de la fenêtre de droite grâce à un système d'onglets très bien pensé.



La console de Gestion ISA version 2004

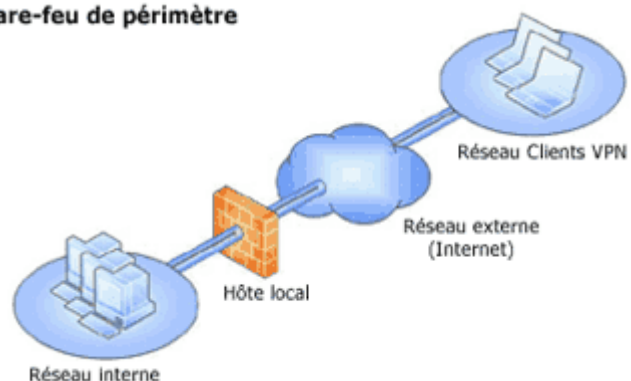
## 2.3 L'assistant modèle réseau

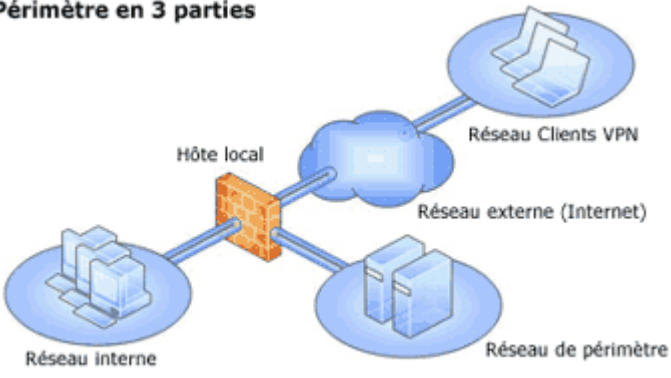
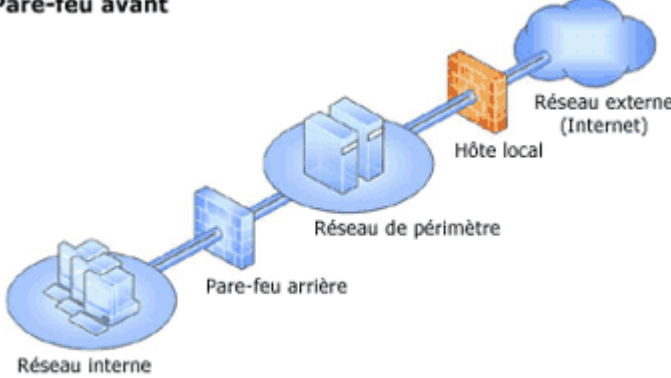
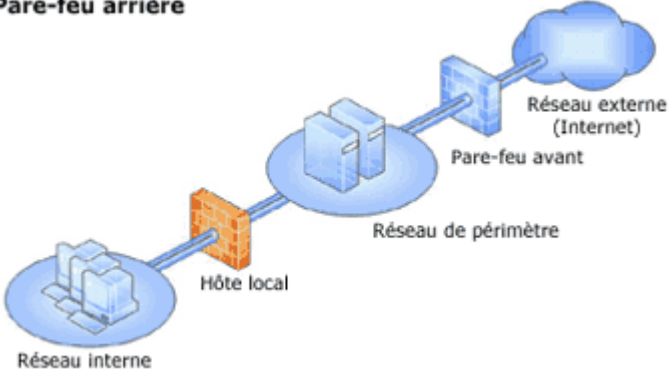
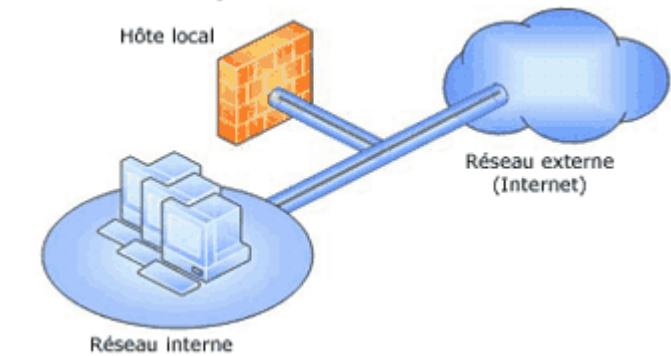
L'une des principales améliorations au niveau de l'interface concerne **la configuration du NAT et/ou routage entre les différents réseaux connectés au serveur ISA**. En effet, un assistant très efficace est désormais disponible pour mettre en place sans efforts administratifs les topologies réseau classiquement utilisées sur un pare-feu. Il suffit de lancer l'assistant et en 3 clics de souris, les règles qui permettent la communication entre les différents réseaux reliés au serveur sont automatiquement paramétrées. Cinq configurations sont prédéfinies :

- **Pare-feu de périmètre**

Dans cette configuration, le serveur ISA est un hôte bastion, c'est-à-dire un pare-feu interconnectant un réseau privé à un réseau public. C'est le scénario classique en entreprise lorsque l'on souhaite filtrer l'accès à Internet.

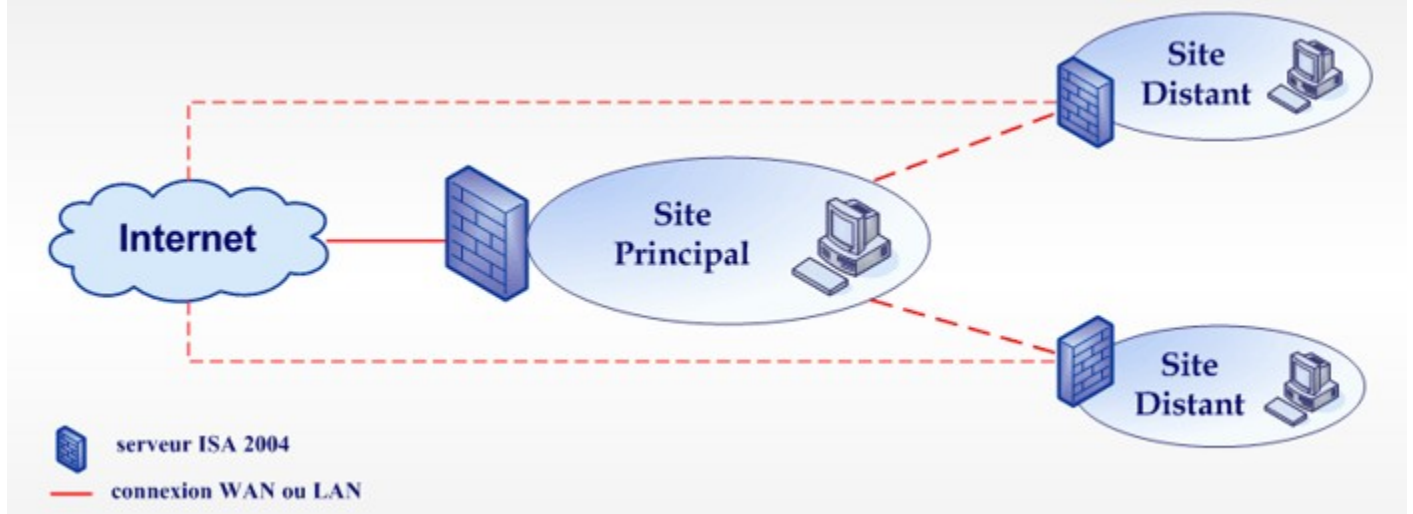
### **Pare-feu de périmètre**



<ul style="list-style-type: none"> <li>• <b><u>Périmètre en trois parties</u></b></li> </ul> <p>Le serveur ISA possède trois interfaces chacune connectée à un sous réseau ou à un réseau différent :</p> <ul style="list-style-type: none"> <li>- la première est connectée au réseau interne de l'entreprise</li> <li>- la seconde à un réseau périphérique encore appelé zone démilitarisée ou DMZ (DeMilitarized Zone)</li> <li>- la dernière à un réseau public comme Internet.</li> </ul>	<p><b>Périmètre en 3 parties</b></p> 
<ul style="list-style-type: none"> <li>• <b><u>Pare-feu avant</u></b></li> </ul> <p>Dans ce scénario, le serveur ISA est configuré pour être le premier pare-feu d'un réseau équipé de deux pare-feu mis dos-à-dos. Le serveur ISA est l'ordinateur qui filtre les informations circulant entre le réseau périphérique (DMZ) et le réseau public (ex. : Internet).</p>	<p><b>Pare-feu avant</b></p> 
<ul style="list-style-type: none"> <li>• <b><u>Pare-feu arrière</u></b></li> </ul> <p>Dans ce scénario, le serveur ISA est configuré pour être le second pare-feu d'un réseau équipé de pare-feu dos-à-dos. Le serveur ISA est l'ordinateur qui filtre les informations circulant entre le réseau interne de l'Entreprise et le réseau Périphérique (DMZ).</p>	<p><b>Pare-feu arrière</b></p> 
<ul style="list-style-type: none"> <li>• <b><u>Carte réseau unique</u></b></li> </ul> <p>Dans cette configuration, ISA Server 2004 est paramétré pour assurer uniquement la fonction de mise en cache (serveur de Proxy). Il fonctionne sur le même réseau que le réseau interne et ne peut faire ni routage, ni serveur VPN, ni pare-feu.</p>	<p><b>Carte réseau unique</b></p> 

Bien entendu l'administrateur du serveur a toujours la possibilité de créer ces règles réseaux et il peut aussi éditer manuellement toute la configuration. Cependant, l'assistant a le mérite de débarrasser l'administrateur de cette tâche supplémentaire ce qui lui permet de se concentrer sur les autres paramètres du serveur dédiés eux à la sécurité (mise en place de règles, d'alertes et de filtres).





 serveur ISA 2004  
 connexion WAN ou LAN  
 [Lien vers la page de configuration VPN](#)  
 **Exporter** les réseaux existants  
 **Importer** des réseaux

Pour accéder à l'onglet ci-contre, il suffit de développer l'arborescence et d'aller dans *configuration/networks*.

## 2.4 Chaînage de pare-feu et chaînage web

Le chaînage consiste à raccorder plusieurs serveurs ISA entres eux afin d'**optimiser au maximum l'utilisation de la bande passante réseau**. Cette fonctionnalité peut se révéler très utile dans le cas d'une entreprise possédant un site principal et plusieurs sites distants. Il existe deux types de chaînage sous ISA Server 2004 :

- le **chaînage web** qui s'applique uniquement aux clients du Proxy web
- le **chaînage de pare-feu** qui s'applique uniquement aux clients SecureNAT et aux clients pare-feu

Considérons une entreprise possédant un site principal et deux sites distants. Admettons que le site principal regroupent environ 2500 machines alors que les succursales en regroupent 50 chacune. Toutes les machines clientes sont configurées en tant que clients du Proxy web. Chaque succursale contient un serveur ISA fonctionnant en tant que serveur de proxy. Dans ce cas, il est possible d'accélérer grandement les performances de la navigation web dans les sites distants de la manière suivante :

- utiliser la connexion Internet locale pour les requêtes HTTP destinées à des sites web français (c'est-à-dire des sites appartenant au domaine DNS \*.fr)
- rediriger toutes les autres requêtes vers le serveurs ISA du site principal afin de bénéficier du fichier de cache de ce serveur qui doit être plus conséquent et plus à jour étant donné le nombre de clients appartenant au site principal.

### le chaînage de serveurs ISA



Le **chaînage web** route (ou redirige) les demandes des clients du Proxy web vers **la connexion Internet locale, un autre serveur de Proxy situé en amont** ou bien directement vers un **serveur HTTP**. ISA Server 2004 permet de définir **des règles de chaînage web** très flexible afin d'optimiser au maximum les performances de la navigation et la charge réseau. On peut par exemple rediriger les requêtes à destination d'une URL ou d'un ensemble d'URL donné vers un serveur de Proxy spécifique.

Réseaux				Ensembles de réseaux				Règles de réseaux				Chaînage Web			
Ordre	Nom			À			Action								
1	accès aux sites hardware			sites de hardware			Rediriger vers site hébergé 172.16.16.3								
2	accès aux sites financiers/bancaires			site de la bourse sites bancaires sites financiers			Rediriger vers le serveur amont 172.64.13.50								
3	accès aux sites du domaine FR			domaine FR			Rediriger vers le serveur amont 172.16.16.1								
Dernier	Règle par défaut			Tous les réseaux (et l'hôte local)			Récupérer directement la demande								

Le **chaînage de pare-feu** redirige les demandes des clients SecureNAT et des clients pare-feu vers **la connexion Internet locale ou vers un autre serveur ISA situé en amont**. Il n'est pas possible de définir de règles précises en ce qui concerne le chaînage de pare-feu

## 3. Paramétrage du pare-feu

### 3.1 Introduction

Nous allons maintenant voir comment paramétrer le pare-feu du serveur ISA. En effet, depuis la version 2000, les options du pare-feu ont été profondément revues. Voici un rappel des nouveautés :

- Interface et méthode de **création des règles d'accès améliorées**
- Modification de **l'ordre d'application des règles**
- **Stratégie système**
- Remaniement des **filtres d'application**

### 3.2 Les éléments de stratégie

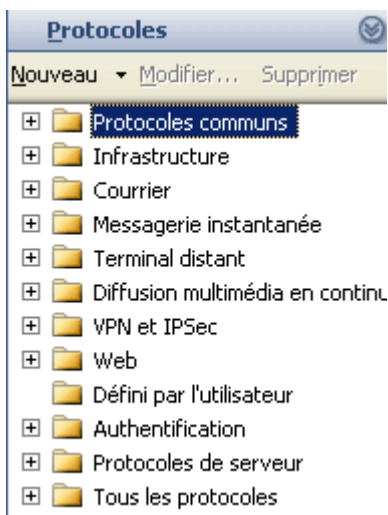
A l'instar d'ISA 2000, on utilise des **éléments de stratégie définis préalablement** afin de simplifier et de structurer la création de règles d'accès pour le pare-feu mais aussi pour la création de tous les autres types de règles existantes (règles de mise en cache, règles de stratégie système,...) comme nous le verrons ultérieurement. Les différents types d'éléments sont :

- **Protocoles**



- **Utilisateurs**
- **Types de contenus**
- **Planifications**
- **Objets de réseau**

Un certain nombre d'éléments existent par défaut ce qui évite à l'administrateur de devoir tous les re-définir. On peut créer et visionner les éléments de stratégie dans l'onglet **boîte à outils** située dans le menu de la fenêtre de droite (ce menu s'affiche si l'on sélectionne **stratégie de pare-feu** dans l'arborescence).



Par défaut **le nombre de protocoles préfinis est impressionnant.**

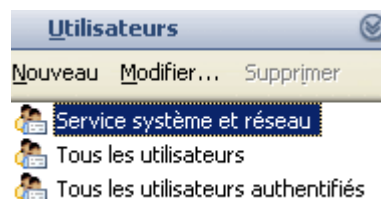
Ils sont classés par groupe ce qui facilite grandement les recherches. Ainsi si l'on souhaite paramétrer une règle pour autoriser ou refuser l'accès aux pages Web il faudra aller chercher dans le conteneur *Web* qui contient notamment les protocoles HTTP et HTTPS.

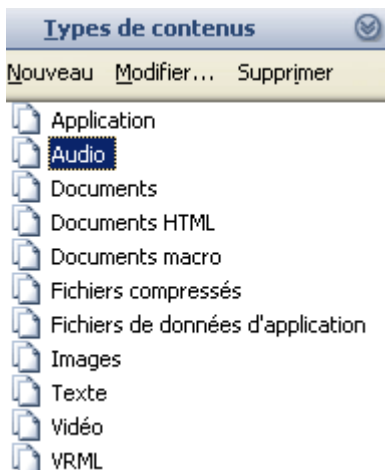
Cette classification se révèle très utile à l'usage. En effet, cela évite de devoir faire des recherches sur Internet lorsqu'on ne connaît pas le numéro de port et/ou les plages de ports utilisées par une application donnée. On peut citer quelques dossiers intéressants :

- **VPN et IPSec** qui permet d'autoriser l'accès VPN (IKE, IPSec, L2TP, PPTP,...)
- **Terminal distant** donne accès aux principaux protocoles d'administration à distance (RDP, Telnet, SSH,...)
- **Messagerie instantanée** qui permet d'autoriser ou d'interdire rapidement l'accès aux principales applications (ICQ, AIM, MSN, IRC...)

Bien entendu on peut rajouter des définitions de protocoles à la liste présente au départ si le besoin s'en fait sentir.

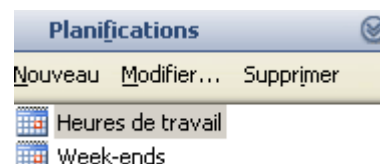
L'onglet **Utilisateurs** permet de créer des groupes d'utilisateurs qui seront utiles lors de la création des règles du pare-feu. La grande nouveauté à ce niveau est la gestion des comptes contenus sur les serveurs **RADIUS** ou sur les serveurs gérant l'authentification via le protocole **SecureID** en plus des comptes de domaine Active Directory.



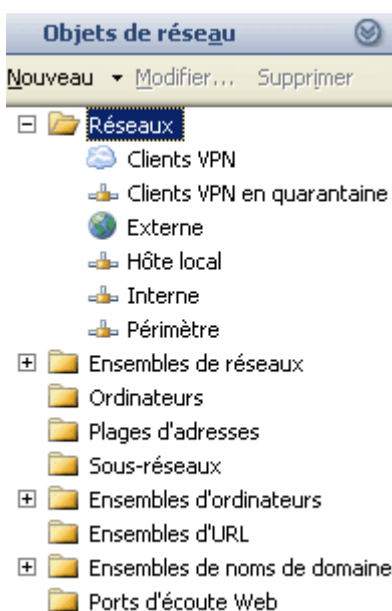


Un certain nombre de types de contenus existe par défaut, ce qui permet de simplifier la création de règles sur les contenus. On peut citer documents **web**, **images**, **audio** ou bien encore **vidéo**. Les éléments de stratégie **Types de contenus** se révèlent très utiles pour permettre à des utilisateurs de surfer tout en les empêchant de télécharger certains fichiers (comme les vidéos par exemple).

Les deux planifications types présentes par défaut sont simplistes et **devront être retouchées** afin de correspondre aux horaires de votre entreprise. Il ne faudra pas hésiter ici à créer **plusieurs autres planifications** comme **pause** ou **repas** qui permettront de paramétrer des règles d'accès spécifiques à certains moments de la journée.



**Les objets réseaux sont très importants** pour le paramétrage des différentes règles du serveur ISA. Les ensembles de réseaux et les réseaux sont créés automatiquement lors de la sélection d'un modèle réseau. Par exemple si vous choisissez le modèle **pare-feu de périmètre** les réseaux **Interne**, **Externe**, **Clients VPN** et **Clients VPN en quarantaine** seront ajoutés. Le réseau **hôte local** est toujours présent, il représente le serveur ISA.



Le "réseau" **clients VPN en quarantaine** contient l'ensemble des clients VPN dont la connexion a été refusée car leurs niveaux de sécurité n'étaient pas satisfaisant. Cette mise en quarantaine des clients "non sécurisés" est une nouveauté de la version 2004 d'ISA server. Nous aborderons la configuration de la mise en quarantaine dans le chapitre dédié au serveur VPN.

Une autre catégorie d'objet de réseau intéressante est la possibilité de créer des **ensembles d'URL** et des ensembles de noms de domaines. Cela va permettre de **bloquer ou d'autoriser certains sites ou certaines pages**. Si le nombre de sites web auquel vos utilisateurs doivent accéder est faible, il est fortement recommandé de créer un élément de stratégie nommé sites autorisés ce qui permettra à vos utilisateurs d'accéder uniquement à ces sites.

### 3.3 La création des règles du pare-feu

Par rapport à sa version 2000, **la création des règles du pare-feu a été modifiée**. Ainsi il n'y a plus qu'un seul type de règles contrairement aux trois types de règles (règles de protocoles, règles de sites et de contenu et filtres de paquets) d'ISA Server 2000. Voici les informations à rentrer pour paramétrer une règle type.

ACTION	PROTOCOLE	SOURCE / DESTINATION	APPLICATION	CONDITION
-refuser -autoriser	ensemble de protocoles port particulier	ensemble de site ensemble de noms de domaine plage d'adresses IPs	utilisateurs groupes personnalisée	plage horaire type de contenu

Cette nouveauté a le mérite de **simplifier la configuration et la compréhension** car on n'a beaucoup moins de règles à paramétrer. Par exemple **pour autoriser l'accès à Internet avec ISA Server 2000 il faut créer deux règles** (une règle de site et de contenu pour autoriser l'accès vers telle ou telle destination et une règle de protocoles pour autoriser les protocoles HTTP et HTTPS) alors qu'**ISA Server 2004 ne nécessite qu'une seule règle** pour arriver au même résultat.



L'onglet **tâches** contient l'ensemble des actions réalisables pour **paramétrer le pare-feu**. On y retrouve les possibilités s'appliquant aux **règles d'accès** (création, édition, désactivation, suppression), mais aussi tous les types de **publication** (publication d'un serveur Web, publication d'un serveur web sécurisé, publication d'un serveur de messagerie, publication de serveur).

On peut de plus afficher, modifier, importer et exporter **les règles de la stratégie système**. Ces règles sont définies automatiquement et s'appliquent spécifiquement au serveur ISA qui correspond au "réseau" **hôte local**. Ces règles permettent par exemple au serveur ISA de **joindre un serveur DHCP ou un contrôleur de domaine**. Les règles de stratégie système sont donc essentielles au bon fonctionnement du serveur ISA.

Le lien **définir les préférences d'IP** permet quand à lui d'activer le **routing IP** et de paramétrer le **filtre d'options IP**. Le filtre d'options IP permet d'autoriser ou de refuser les paquets possédant des options spécifiques.

Toutes les opérations **d'importation et d'exportation** utilisent le **format XML**.

Des **exemples de création de règles d'accès** sont présentés dans [la partie dédiée à cet effet](#).

### 3.4 Ordre d'application des règles

Avec ISA Server 2000, lorsqu'une requête arrive au pare-feu, une procédure spécifique pour autoriser ou refuser le passage de la requête est réalisée :

1. Vérification de l'existence d'**une règle de site et de contenu qui refuse la requête**
2. Vérification de l'existence d'**une règle de site et de contenu qui autorise explicitement la requête**

3. Vérification de l'existence d'**une de protocole qui refuse la requête**
4. Vérification de l'existence d'**une de protocole qui autorise explicitement la requête**
5. Vérification de l'application d'**un éventuel filtre de paquet**

Avec la nouvelle version, cette procédure complexe est remplacée par un autre système. **Dorénavant, chaque règle possède un numéro et lorsqu'une requête arrive au serveur, c'est la règle qui a le numéro le plus faible qui s'applique.** Ce système a le mérite d'être beaucoup **plus simple** à comprendre que l'ancien et il est d'ailleurs repris en ce qui concerne l'ensemble des règles que l'on peut créer avec ISA Server 2004 (**règles de translation d'adresse et de routage, règles de pare-feu, règles de cache, ...**). Voici un exemple de règles que l'on peut paramétrer :

Stratégie de pare-feu						
Ordre	Nom	Action	Protocoles	De / Port d'écoute	À	Condition
1	interdire l'accès aux sites de recherche	Refuser	HTTP;...	Interne	sites de recherche	Tous les utilisateurs
2	autoriser l'accès à Internet	Autoriser	FTP;HT...	Interne	Externe	Tous les utilisateurs...
	Dernier Règle par défaut	Refuser	Tout le...	Tous les rése...	Tous les rése...	Tous les utilisat...

On note la présence d'**une règle spécifique ne portant pas de numéro et notée : «Dernier »**. Comme vous pouvez le voir sur la capture d'écran ci-dessus, **cette règle bloque tous les protocoles de toutes les sources vers toutes les destinations**. Elle est toujours située à la fin et possède donc la priorité la plus basse.

### 3.5 Les règles de stratégie système

La **stratégie système** est un ensemble de règles qui permettent au serveur ISA de **joindre certains services réseau fréquemment utilisés**. Au premier abord, on pourrait considérer ces règles de stratégie système comme **un trou de sécurité**. Cependant la plupart de ces règles autorisent juste la communication entre l'hôte local et le réseau interne. En aucun cas, un utilisateur externe ne peut accéder au serveur ISA ou bien au réseau de l'entreprise via l'une de ces règles. Le but de Microsoft avec la stratégie système est de trouver un bon compromis entre connectivité et sécurité.

Si la stratégie système n'existait pas, **le serveur ISA ne pourrait communiquer avec aucune autre machine**. Ceci empêcherait notamment le serveur ISA de réaliser les actions suivantes :

- ouvrir une session sur le domaine
- récupérer un bail DHCP
- résoudre les noms de domaines pleinement qualifié en adresse IP
- etc.

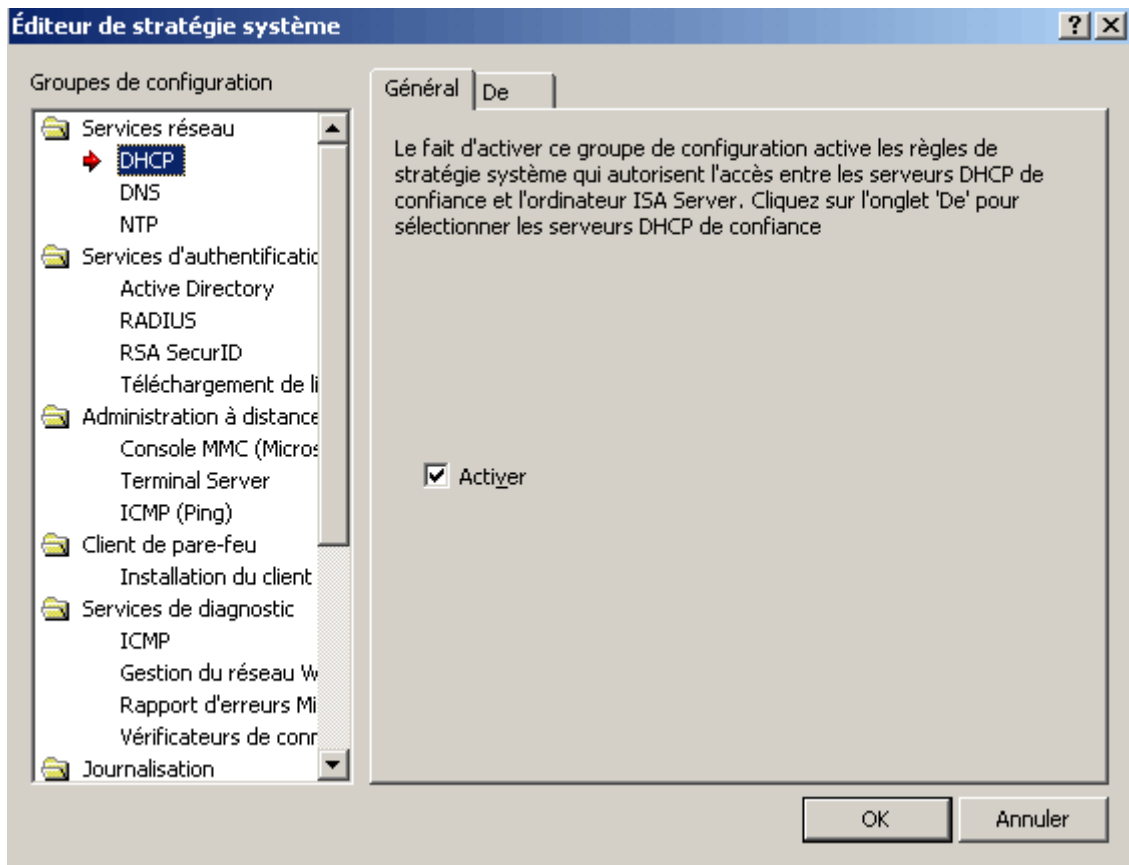
Le scénario de **l'installation à distance via une session Terminal Server** permet de bien se rendre compte de l'utilité de la stratégie système du point de vu administratif. En effet, si la stratégie système n'existait pas, vous pourriez installer ISA 2004 sur une machine distante, mais dès le lancement du service pare-feu, **la session Terminal Server serait immédiatement déconnectée** car le protocole RDP serait bloqué. Cela obligerait ensuite l'administrateur à se déplacer sur le site

distant pour créer une règle d'accès autorisant le protocole RDP ce qui peut s'avérer contraignant si le site distant est situé à 6000 kilomètres !

Stratégie de pare-feu					
O...	Nom	Action	Protocoles	De / Port d'éco...	À
<b>Règles de stratégie système</b>					
1	Autoriser l'accès aux services d'annuaire dans u...	Autoriser	LDAP LDAP (UDP) LDAP GC (catalogue global) LDAPS LDAPS GC (catalogue global)	Hôte local	Interne
2	Autoriser l'administration à distance depuis les o...	Autoriser	Contrôle Pare-feu Microsoft Datagramme NetBios Nom de service NetBios RPC (toutes interfaces) Session NetBios	Ordinateurs ...	Hôte local
3	Autoriser l'administration à distance depuis les o...	Autoriser	RDP (services Terminal Ser...	Ordinateurs ...	Hôte local
4	Autoriser la journalisation à distance vers les ser...	Autoriser	Datagramme NetBios Nom de service NetBios Session NetBios	Hôte local	Interne
5	Autoriser l'authentification RADIUS depuis ISA S...	Autoriser	Gestion de comptes RADIUS RADIUS	Hôte local	Interne
6	Autoriser l'authentification Kerberos depuis ISA ...	Autoriser	Kerberos-Sec (TCP) Kerberos-Sec (UDP)	Hôte local	Interne
7	Autoriser DNS depuis ISA Server vers les serveu...	Autoriser	DNS	Hôte local	Tous les ré..
8	Autoriser les demandes DHCP depuis le serveur ...	Autoriser	DHCP (demande)	Hôte local	Partout
9	Autoriser les demandes DHCP depuis ISA Server ...	Autoriser	DHCP (réponse)	Interne	Hôte local
10	Autoriser les demandes ICMP (PING) depuis les ...	Autoriser	Ping	Ordinateurs ...	Hôte local
11	Autoriser les demandes ICMP depuis ISA Server ...	Autoriser	Demande d'informations ICMP Horodateur ICMP Ping	Hôte local	Tous les ré..

extrait des règles de stratégie système

Bien entendu, **les règles de stratégie système inutiles doivent être désactivées** afin de réduire la surface d'attaque. Pour ce faire, un assistant spécifique nommé **Éditeur de stratégie système** est disponible. Il permet de désactiver toutes les règles de stratégie système, mais aussi de les configurer.



L'éditeur de stratégie système est accessible à partir de l'onglet **Tâches**

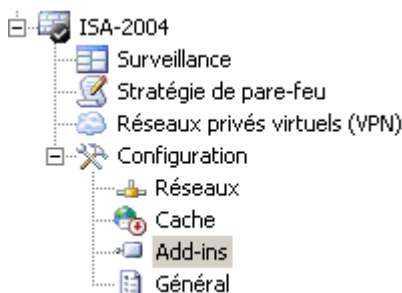
### 3.6 Le filtrage applicatif

Cette nouvelle version d'ISA Server met l'accent sur les **filtres d'application** qui sont maintenant plus nombreux et qui possèdent des fonctionnalités avancées. Contrairement aux filtres de paquets qui analysent uniquement l'en-tête des paquets IP pour savoir si le paquet doit être bloqué ou non, **les filtres d'application analysent aussi le corps du paquet**. Les filtres d'application sont au nombre de 12.



Nom	Description	Fournisseur	Version
• Filtre d'accès FTP	Active les protocoles FTP (client et serveur)	Microsoft (R) Corp...	4.0
• Filtre de détection d'intrusion POP	Recherche les attaques par dépassement de ta...	Microsoft (R) Corp...	4.0
• Filtre de proxy Web	Active le proxy et le cache HTTP	Microsoft (R) Corp...	4.0
• Filtre DNS	Filtre le trafic DNS	Microsoft (R) Corp...	4.0
• Filtre H.323	Activer le protocole H.323	Microsoft (R) Corp...	4.0
• Filtre MMS	Active le protocole de flux de média Microsoft	Microsoft (R) Corp...	4.0
• Filtre PNM	Active le protocole diffusion multimédia en conti...	Microsoft (R) Corp...	4.0
• Filtre PPTP	Active le tunnel PPTP via ISA Server	Microsoft (R) Corp...	4.0
• Filtre RPC	Active la publication des serveurs RPC	Microsoft (R) Corp...	4.0
• Filtre RTSP	Active le protocole de flux en temps réel	Microsoft (R) Corp...	4.0
• Filtre SMTP	Filtre le trafic SMTP	Microsoft (R) Corp...	4.0
• Filtre SOCKS v4	Active la communication SOCKS 4	Microsoft (R) Corp...	4.0

### exemple de filtres d'application



Pour activer ou désactiver des filtres d'application, il faut utiliser la fenêtre présentée ci-dessus (cette fenêtre est située dans le menu configuration / Add-ins de l'arborescence). **Par défaut tous les filtres d'application sont activés afin de procurer une sécurité maximale.** Les filtres inutilisés peuvent être désactivés afin de ne pas faire chuter les performances sur une machine peu puissante.

## 3.7 Conclusion

Voici les points essentiels à retenir pour créer des règles d'accès sous ISA Server 2004 :

- La création des règles d'accès fait appel à des **éléments de stratégie**
- Chaque règle est appliquée dans **un ordre bien précis**
- Des **filtres spécifiques** peuvent être appliqués sur les règles d'accès
- Certaines règles sont présentent par défaut (**stratégie système**)



# 4. Exemples de configuration

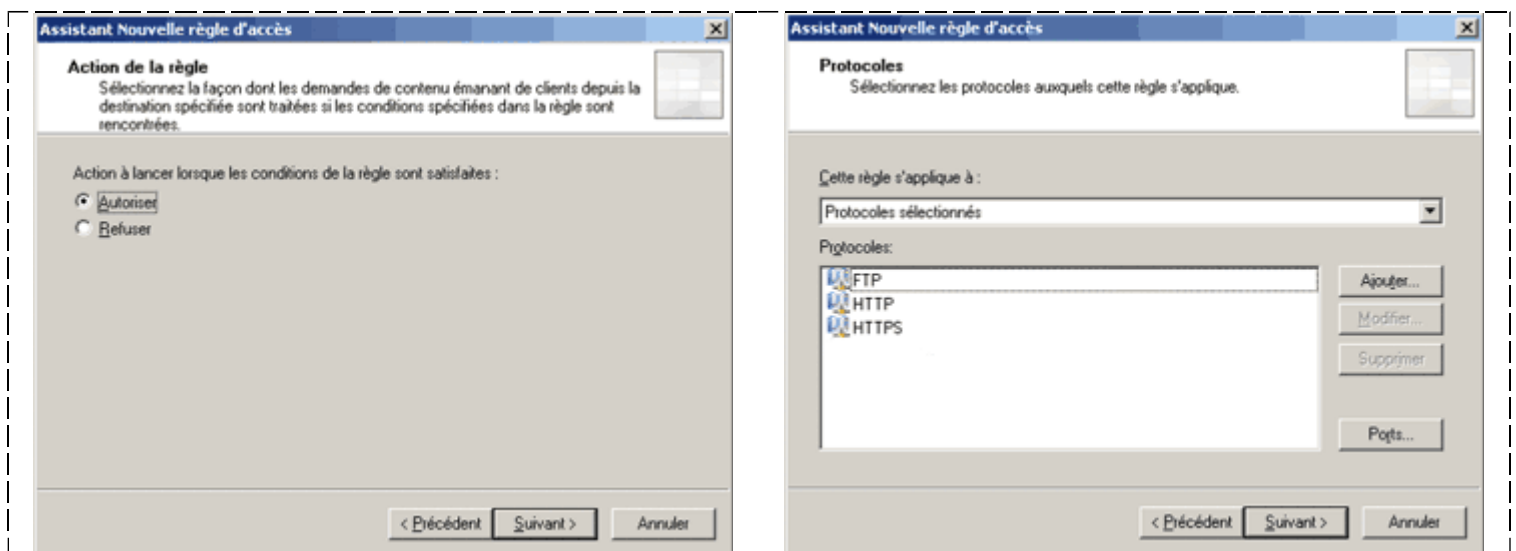
## 4.1 Introduction

Ce chapitre a pour but de présenter la configuration de certaines règles souvent mises en place (accès à Internet, autorisation/interdiction de MSN Messenger, ...). Chaque sous partie se consacre à un exemple en particulier.

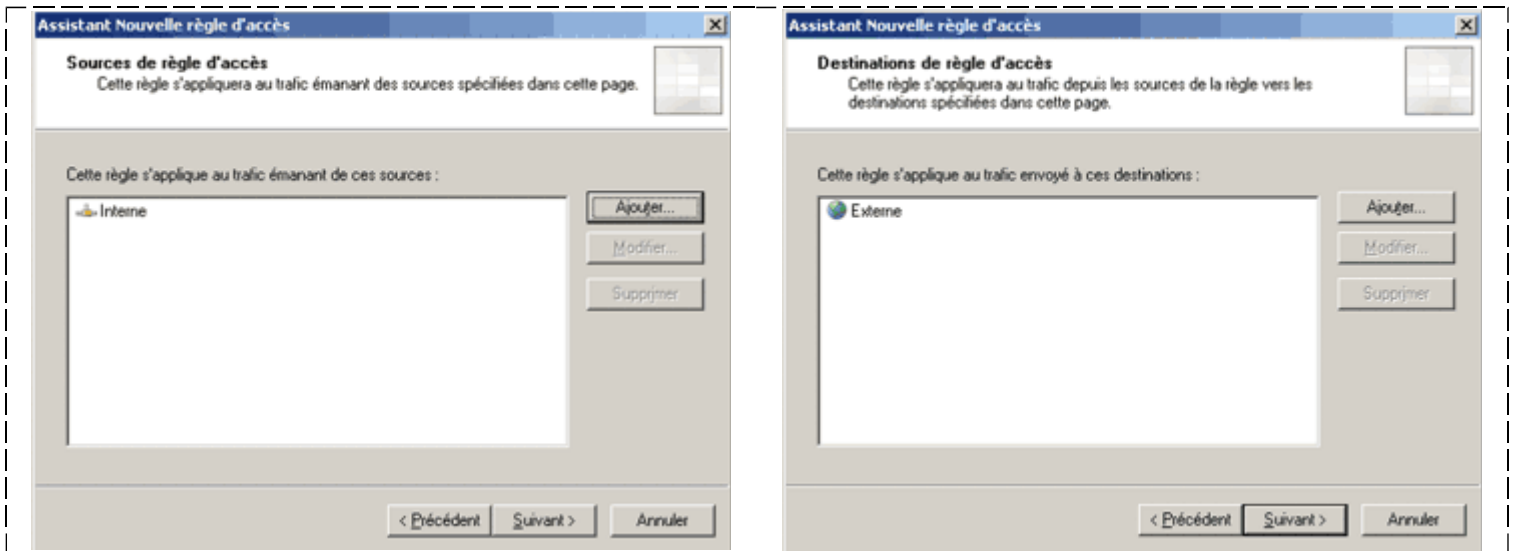
## 4.2 Autoriser l'accès à Internet pour les clients du réseau interne

Nous allons maintenant créer **une règle autorisant l'accès à Internet** (c'est-à-dire au réseau externe dans cet exemple) pour tous les clients pare-feu du réseau interne via le ports 21, 80, 443 et 1863 (le port utilisé par MSN Messenger pour la connexion et l'échange de messages).

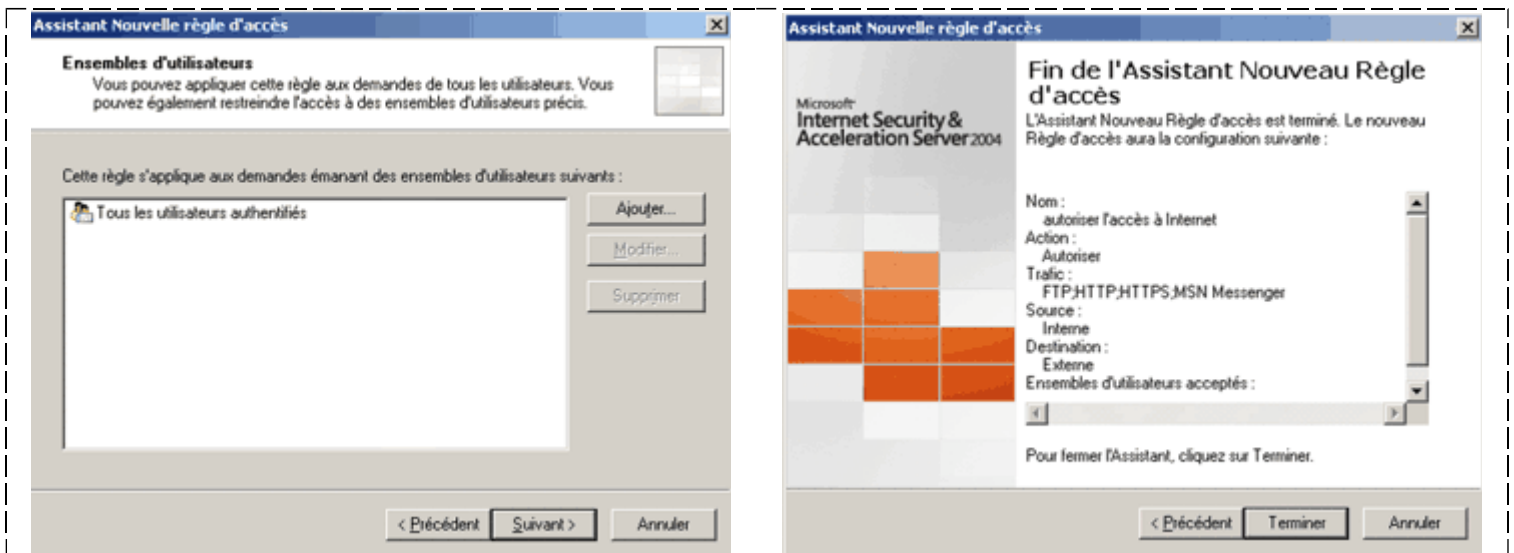
Il faut commencer par donner **le nom le plus explicite possible** à la règle que l'on souhaite créer. On doit ensuite sélectionner **l'action à effectuer (autoriser ou refuser)**. Si l'on sélectionne Refuser, la possibilité de rediriger la requête vers une page web est offerte (cela permet de faire comprendre à l'utilisateur que la page a été bloquée intentionnellement par le pare-feu et que ce n'est donc pas un problème technique). Il faut choisir le ou les ports de destination pour le(s)quel(s) la règle va s'appliquer. Dans notre exemple, tous les protocoles sont prédéfinis (ce sont des éléments de stratégie présent par défaut dans le serveur) et il suffit juste d'ajouter **les protocoles nommés FTP, HTTP et HTTPS** à l'aide du bouton adéquat. Il est possible de **définir quels sont les ports** sources à l'aide du bouton **Ports...** Dans notre exemple nous laissons l'option par défaut qui autorise tous les ports sources (ainsi les clients pourront accéder à des sites web et à des serveurs FTP quel que soit le logiciel client utilisé).



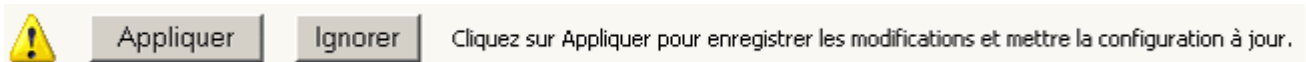
L'étape suivante consiste à **spécifier le réseau source et le réseau de destination**. Dans notre exemple, le réseau source correspond à **Interne** (le réseau local de l'entreprise) et le réseau de destination correspond à **Externe** (Internet).



Enfin on sélectionne les **ensembles d'utilisateurs** pour lesquels la règle entrera en action. Dans notre cas, le groupe nommé **Tous les utilisateur authentifiés** est retenu. Cependant, tous les groupes de sécurité définis dans le service d'annuaire Active Directory peuvent être utilisés pour créer une règle plus fine.



Une fois l'assistant terminé, la règle est inopérante. Pour que qu'elle entre en action il suffit de cliquer sur le bouton **Appliquer** qui apparaît au milieu de l'interface de la console de gestion ISA.



Et voilà ! **Tous les utilisateurs de votre réseau ont maintenant accès à Internet**, et ce quel que soit leur navigateur (Internet Explorer, Safari, Firefox, Opéra,...) ou bien leur client FTP (Internet Explorer, FileZilla,...). Bien entendu, **certain pré-requis doivent être respectés** pour que tout fonctionne correctement :

- Les ordinateurs clients doivent être capable de **joindre un serveur DNS** résolvant les noms DNS "publiques"
- Les ordinateurs client doivent être configurés pour **joindre le serveur ISA**

- Le **pare-feu** présent sur les ordinateurs client doit lui aussi être configuré pour autoriser l'accès à Internet

#### 4.3 Interdire complètement l'accès à MSN Messenger

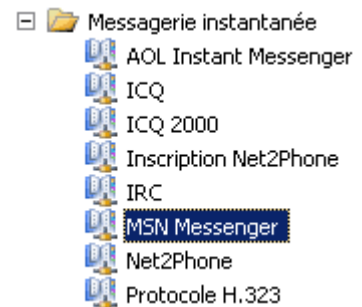
A l'instar de Windows Messenger, MSN Messenger est une **application de messagerie instantanée** permettant d'accroître grandement la productivité des utilisateurs (chat, vidéoconférence, échange de fichiers aisé,...). Cependant l'utilisation de ce logiciel en entreprise peut entraîner quelques dérives... Si vous souhaitez empêcher certains utilisateurs de l'utiliser, plusieurs solutions sont envisageables :

- **créer deux règles d'accès** interdisant la communication avec le serveur messenger.hotmail.com
- **configurer les clients pare-feu** pour empêcher MSN Messenger d'accéder au réseau
- **configurer le filtre HTTP** pour bloquer l'application MSN Messenger en analysant le paramètre adéquat

Nous allons étudier les avantages et les inconvénients de chacune de ces méthodes.

##### 1ère méthode

Étant donné que **MSN Messenger utilise plusieurs ports** ou plage de ports pour mettre en oeuvre ses différents services (texte, échange de fichier, son...). La solution la plus simple reste d'**interdire le port TCP 1863** qui est utilisé pour l'échange de messages textuels mais surtout pour **la connexion initiale**. Pour cela, il n'est pas nécessaire de créer un élément de stratégie, puisque le protocole MSN Messenger est prédéfini dans ISA 2004. Il suffit donc de **créer une règle d'accès bloquant le protocole MSN Messenger** entre le réseau **Interne** et le réseau **Externe** et s'appliquant au bon groupe d'utilisateurs.

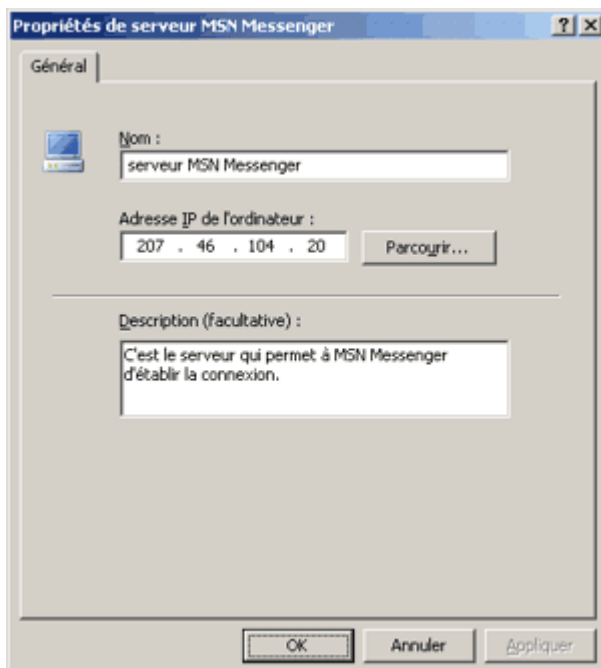


Cependant, une fois la règle d'accès correctement créée, **tous les utilisateurs peuvent encore utiliser MSN Messenger !!!** La connexion est un peu plus lente (environ 10 secondes d'écart), mais s'effectue tout de même, ce qui permet à des utilisateurs non autorisés de "chatter". Une bonne méthode dans un cas comme celui-ci, est d'utiliser un programme pour **analyser les trames** envoyées par le logiciel MSN Messenger afin de mieux comprendre son fonctionnement. Il existe pour cela des outils gratuits tels que le **Moniteur réseau Microsoft** ou bien encore **Ethereal**. Voici les résultats d'une analyse de trames lancée au moment où l'utilisateur clique sur le bouton **Ouvrir une session...**

No.	Time -	Source	Destination	Protocol	Info
1	0.000000	10.1.0.2	207.46.104.20	TCP	1245 > 1863
2	2.928482	10.1.0.2	207.46.104.20	TCP	1245 > 1863
3	8.946299	10.1.0.2	207.46.104.20	TCP	1245 > 1863
4	10.021986	10.1.0.2	207.46.104.20	TCP	1246 > http

On remarque que le logiciel (exécuté sur une machine dont l'adresse IP est 10.1.0.2) essaye de **se connecter au serveur 207.46.104.20** (cette adresse correspond au FQDN messenger.hotmail.com) en utilisant le port 1863 du protocole TCP. L'opération est répétée **trois fois consécutives** si le serveur ne répond pas immédiatement. Ce port étant bloqué au niveau du pare-feu, la demande n'aboutit jamais. L'application essaye ensuite dans un second temps de se connecter à ce même

serveur mais à l'aide du port 80 qui est normalement réservé au protocole HTTP. Ce port étant ouvert au niveau du pare-feu afin de permettre la navigation web, l'application réussit à se connecter et la session de l'utilisateur peut ensuite s'ouvrir.



Ce problème peut se résoudre à l'aide d'une règle d'accès interdisant la communication entre les machines du réseau **Interne** et le serveur **messenger.hotmail.com**. Pour cela il faut créer au préalable un élément de stratégie pointant vers **l'adresse IP** du serveur messenger.hotmail.com ou bien directement vers le **nom de domaine pleinement qualifié** messenger.hotmail.com. **Il est plus judicieux d'interdire le FQDN** car même en cas de modification de l'adresse IP du serveur la règle restera valide. La fenêtre ci à gauche montre les propriétés d'un élément de stratégie. Il se nomme **serveur MSN Messenger** et pointe vers l'adresse IP **207.46.104.20**.

Une fois l'élément de stratégie correctement configuré, il suffit de créer une règle **refusant les connexions au domaine messenger.hotmail.com** et s'appliquant aux **groupes appropriés**. Bien entendu, on peut altérer la règle précédemment créée pour **bloquer le port 1863** en ajoutant le protocole **HTTP** au protocole **MSN Messenger** et en précisant que la destination est serveur MSN Messenger. Cette règle va donc empêcher les paquets IP expédiés par le réseau Interne et à destination du serveur messenger.hotmail.com d'atteindre leur objectif quel que soit le port utilisé (1863 ou 80).

Dans l'exemple ci-dessous les utilisateurs appartenant aux groupes **Comptabilité, Production ou Recherche** ne peuvent plus se connecter à l'aide du logiciel MSN Messenger.

Stratégie de pare-feu						
O...	Nom	Action	Protocoles	De / Port d'éco...	À	Condition
1	bloquer MSN Messenger	Refuser	HTTP MSN Messenger	Interne	serveur MSN Messenger	Comptabilité Production Recherche

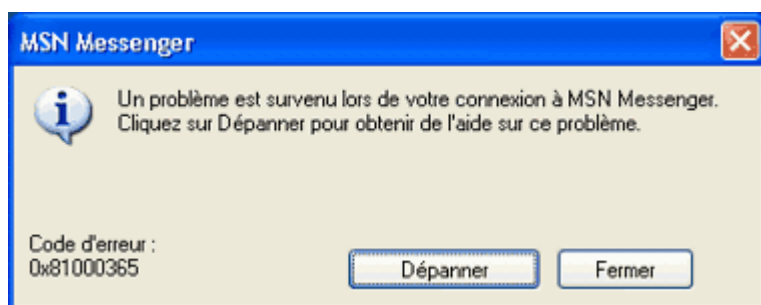
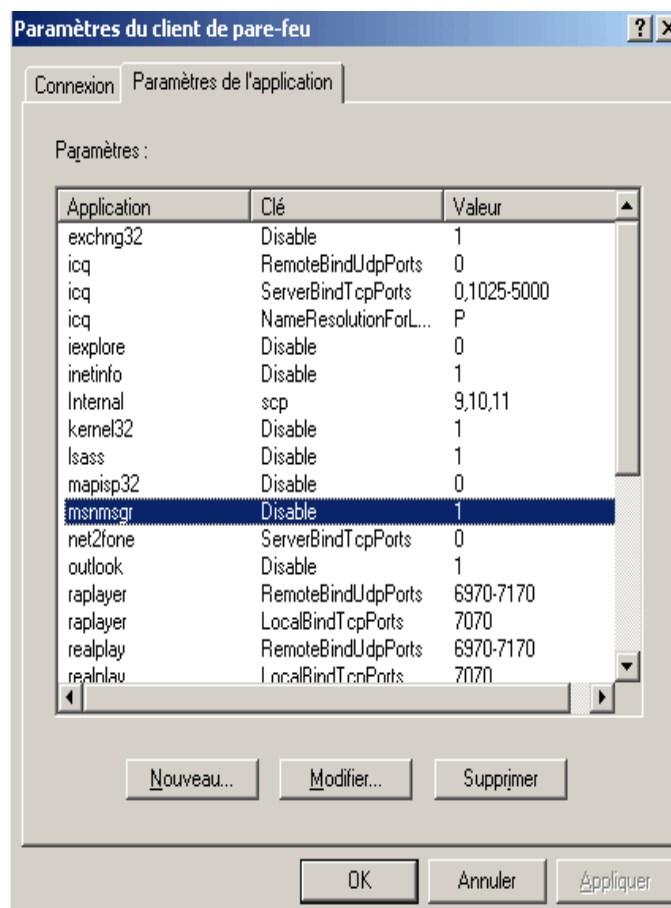
Cette première méthode est celle qui répond le mieux à la problématique car elle demande **peu de ressources** et reste **simple à mettre en œuvre**.

## 2ème méthode

Les clients pare-feu récupèrent à chaque démarrage **une liste des logiciels autorisés ou non à accéder au réseau** (lorsqu'un logiciel n'est pas mentionné dans cette liste il peut tout de même accéder au réseau). Il est possible de bloquer MSN Messenger par ce biais.

Il suffit d'ouvrir la fenêtre **Paramètre du client de pare-feu** située en utilisant le conteneur **Général** de l'arborescence de la console de gestion ISA. Cette fenêtre montre toutes les applications pour lesquelles l'accès au réseau a été configuré. Pour bloquer une application, il suffit d'ajouter **une entrée correspondante au nom du processus** lancé par cette application (sans son extension), puis de **donner la valeur 1 au paramètre Disable**. Dans notre exemple le processus utilisé par MSN Messenger est **msnmsgr.exe**. Il faut donc créer une entrée nommée **msnmsgr**.

Une fois la modification appliquée au niveau du serveur, il faut penser à **redémarrer le service Agent du client de pare-feu** à l'aide des commandes **net stop fcwagent** et **net start fcwagent** (ou bien en utilisant la console **Services**). Dès que cette opération est effectuée, le programme ne peut plus accéder au réseau et la fenêtre ci-dessous apparaît :



Cette méthode est très rapide à mettre en oeuvre et est très efficace. Cependant elle possède **deux inconvénients majeurs** :

- elle **ne s'applique qu'aux clients de pare-feu** (et pas aux clients SecureNAT et clients du proxy web)
- elle **ne permet pas d'interdire l'utilisation du logiciel à des utilisateurs donnés** (tous les utilisateurs seront affectés par l'interdiction d'utilisation)

## 3ème méthode

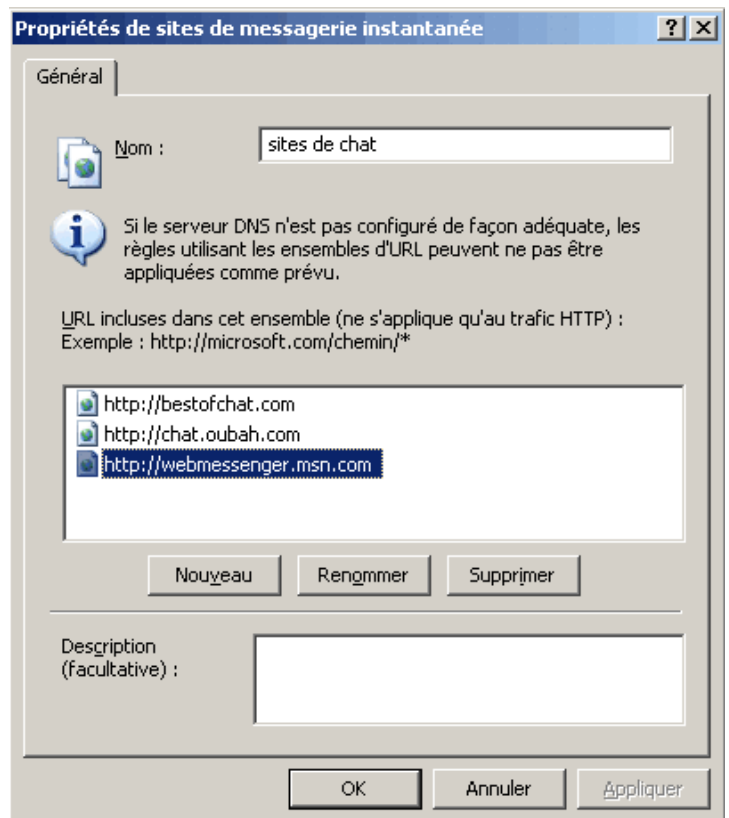
Une dernière méthode consiste à utiliser un filtre web (le filtre HTTP en l'occurrence). C'est le procédé **le plus optimisé et le plus sûr**, cependant, il a le gros inconvénient de demander **énormément de ressources système** au serveur ISA. En effet, lorsque le filtrage web est activé, **le serveur ISA analyse l'en-tête et/ou le contenu de chaque paquet IP** provenant du réseau **Interne** et à destination du réseau **Externe**. C'est pourquoi il faut tenir compte des capacités matérielles du serveur avant d'activer cette option. Le thème du filtrage applicatif et du filtrage web étant trop vaste, nous ne détaillerons pas ici la configuration du **filtre HTTP**.

méthode utilisée	Filtre HTTP	Règle d'accès	Configuration du client pare-feu
besoin en ressources sur le serveur ISA	très fort	faible	quasi nul
type de clients supportés	pare-feu secureNAT proxy web	pare-feu secureNAT proxy web	pare-feu
possibilité d'interdire l'usage du logiciel à un groupe donné ?	oui	oui	non
rapidité de mise en place	long (difficile à configurer et à tester)	rapide	assez long (il faut relancer le service agent du client de pare-feu sur l'ensemble des clients)

Avantages et inconvénients des trois méthodes

#### 4.4 Interdire l'accès à MSN Web Messenger

Une fois le logiciels MSN Messenger bloqué, **les utilisateurs peuvent toujours accéder à ce service par le biais de sa version web**. En effet, le site <http://webmessenger.msn.com/> propose une interface reprenant la plupart des services de la version logicielle. Il peut donc s'avérer utile de bloquer l'accès à cette URL en complément de la désactivation de l'application. Pour cela il suffit de **créer une règle interdisant le trafic entre le réseau interne et le domaine webmessenger.hotmail.com sur le port 80** en TCP. Bien entendu, on peut tout aussi bien bloquer l'URL <http://webssenger.msn.com> ou bien directement l'adresse IP (ci-contre l'ensemble de stratégie nommé **sites de chat** peut être utilisé pour interdire l'accès à webmessenger.msn.com).



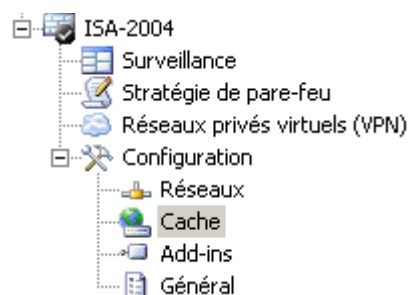
#### 4.5 Conclusion

Certaines règles ne sont pas évidentes à configurer, il faut parfois utiliser des **connexions secondaires** ou des **éléments de stratégie supplémentaire**. Certains logiciels devant être autorisés ou interdit sont parfois pas ou peu documentés. Une bonne méthode permettant de trouver les informations manquantes reste **l'utilisation d'un analyseur de trames** comme le **Moniteur réseau Microsoft** ou bien encore **Ethereal**.

## **5. Implémentation de la mise en cache**

## 5.1 Introduction

ISA Server 2004 joue aussi le rôle de **serveur de proxy**. Tous les paramètres relatifs à la **mise en cache** se configurent dans une fenêtre spécifique accessible via l'arborescence principale (*configuration / cache*).



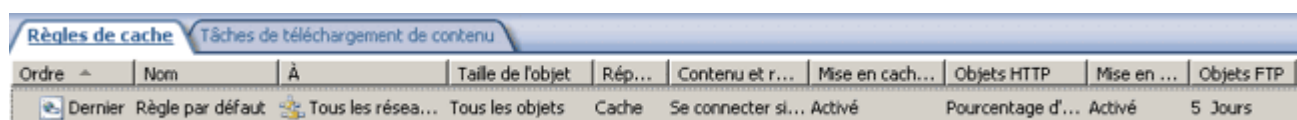
## 5.2 Configuration de la mise en cache



Un onglet "taches" récapitule les diverses actions possibles :

- o **activer/désactiver** la mise en cache
- o créer des **règles de cache** en utilisant les éléments de stratégie prédéfinis
- o **importer/exporter** les règles de cache
- o activer/désactiver et paramétrer la **mise en cache active**

Les règles de cache s'appliquent avec le même système que les règles d'accès et que les règles de stratégie système. La règle qui possède le numéro le plus faible sera donc traitée en priorité. Il existe une **règle par défaut** qui met en cache tous les types **d'objets HTTP et FTP** demandés quel que soit le réseau source. Il est aussi possible de **planifier le téléchargement** de certains contenus dans un onglet spécifique.

L'image capture un tableau des règles de cache. Le tableau a une barre d'onglets avec 'Règles de cache' et 'Tâches de téléchargement de contenu'. Le tableau lui-même a les colonnes suivantes : 'Ordre', 'Nom', 'À', 'Taille de l'objet', 'Rép...', 'Contenu et r...', 'Mise en cach...', 'Objets HTTP', 'Mise en ...', et 'Objets FTP'. Une seule règle est visible : 'Règle par défaut' (Ordre 1), 'À : Tous les résea...', 'Taille de l'objet : Tous les objets', 'Rép... : Cache', 'Contenu et r... : Se connecter si...', 'Mise en cach... : Activé', 'Objets HTTP : Pourcentage d...', 'Mise en ... : Activé', et 'Objets FTP : 5 Jours'.

Les paramètres de la mise en cache restent les mêmes que sur ISA Server 2000 comme le montrent les deux captures d'écran ci-dessous :



## 5.1.Activation du Cache HTTP

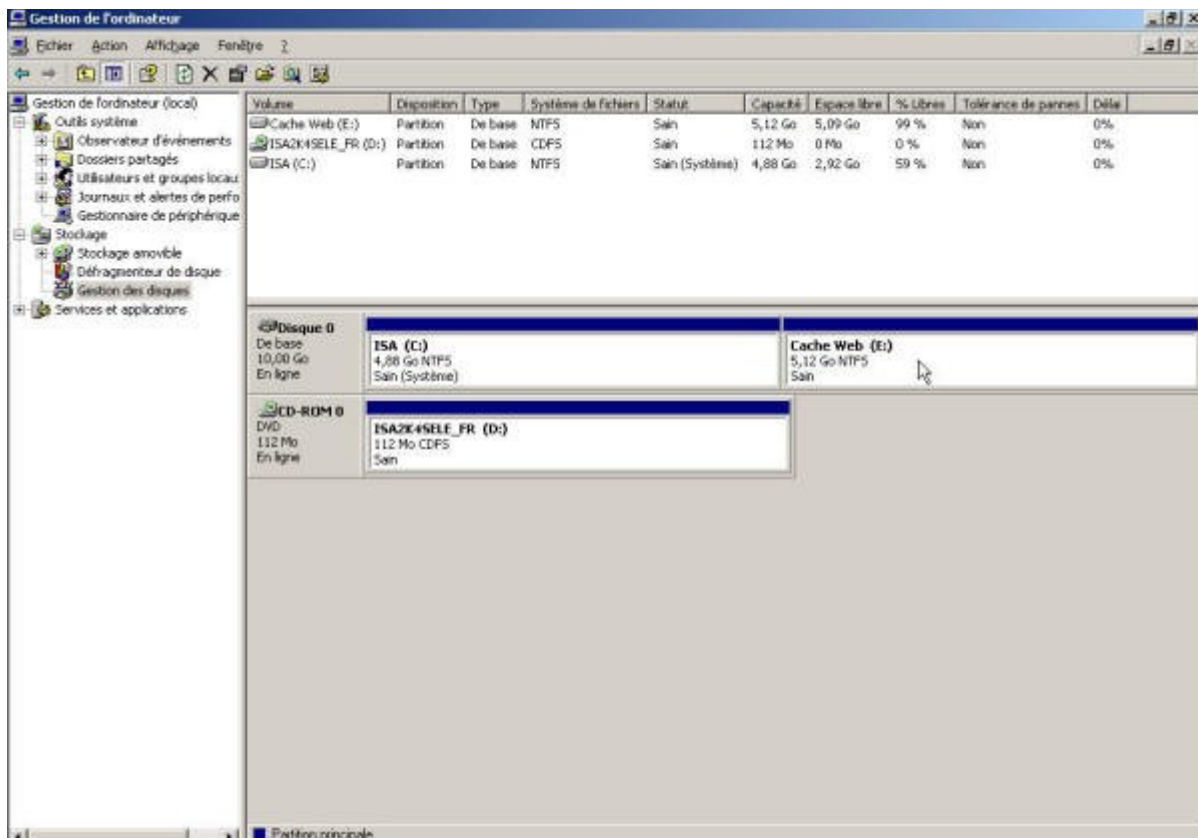
Afin d'améliorer l'affichage des requêtes WEB, ISA Server met en cache les objets fréquemment demandés. Nous allons voir comment mettre en place le cache et le configurer afin de déterminer quel contenu devra être stocké et automatiser la mise en cache.

### 5.1.1. Créer le lecteur du Cache HTTP

Faites un clic droit sur **Poste de travail**, puis sélectionnez **Gérer**.

La console « Gestion de l'ordinateur » s'ouvre. Dans l'arborescence de la console, déroulez le menu « **Stockage** » puis cliquez sur **Gestion des disques**.

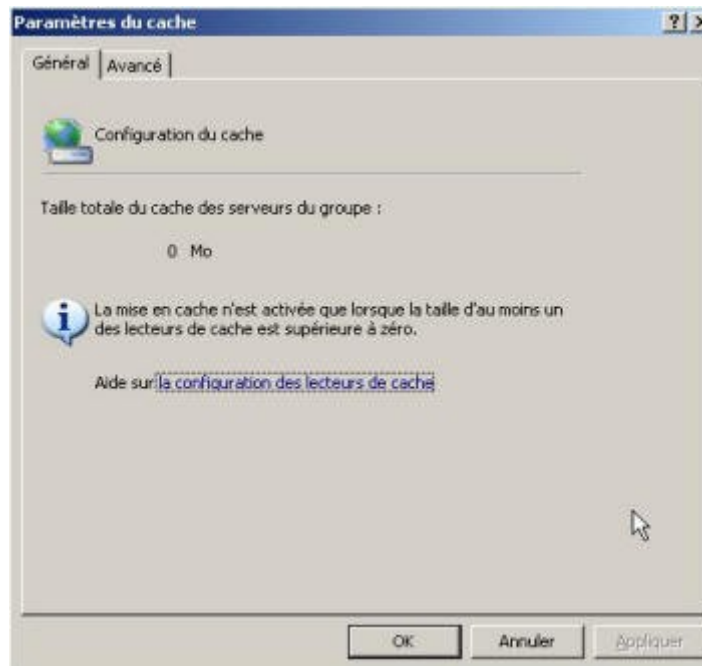
Vous devez disposer d'espace libre sur un de vos disques afin de créer la partition qui servira de Cache HTTP. Faites un clic droit sur votre espace libre puis formater en utilisant le système de fichier NTFS. Donnez à la partition un nom explicite.



Fermez la console

## 5.1.2. Définir les lecteurs de Cache

Faites un clic droit sur **Cache** puis cliquez sur **Propriétés**. La fenêtre « Paramètres du cache » s'ouvre.



Remarquez que **la mise en cache n'est pas activée**, de ce fait, la taille totale du cache est égale à 0 Mo. Cliquez sur « **OK** »

Sélectionnez l'onglet Lecteurs de cache et faites un clic droit sur le volume approprié puis cliquez sur **Propriétés**.

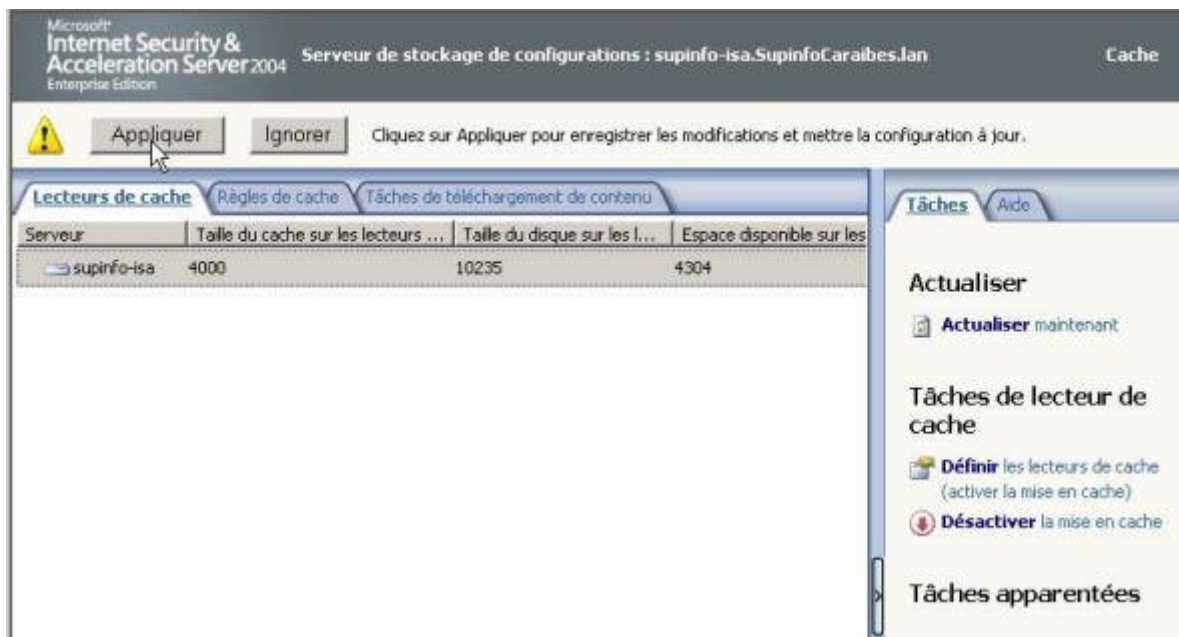


La fenêtre « Propriétés » s'ouvre. **Sélectionnez le lecteur de cache** que vous souhaitez définir puis indiquez la taille maximale (en Mo) du cache choisi, cliquez sur **Définir** puis sur **OK**.

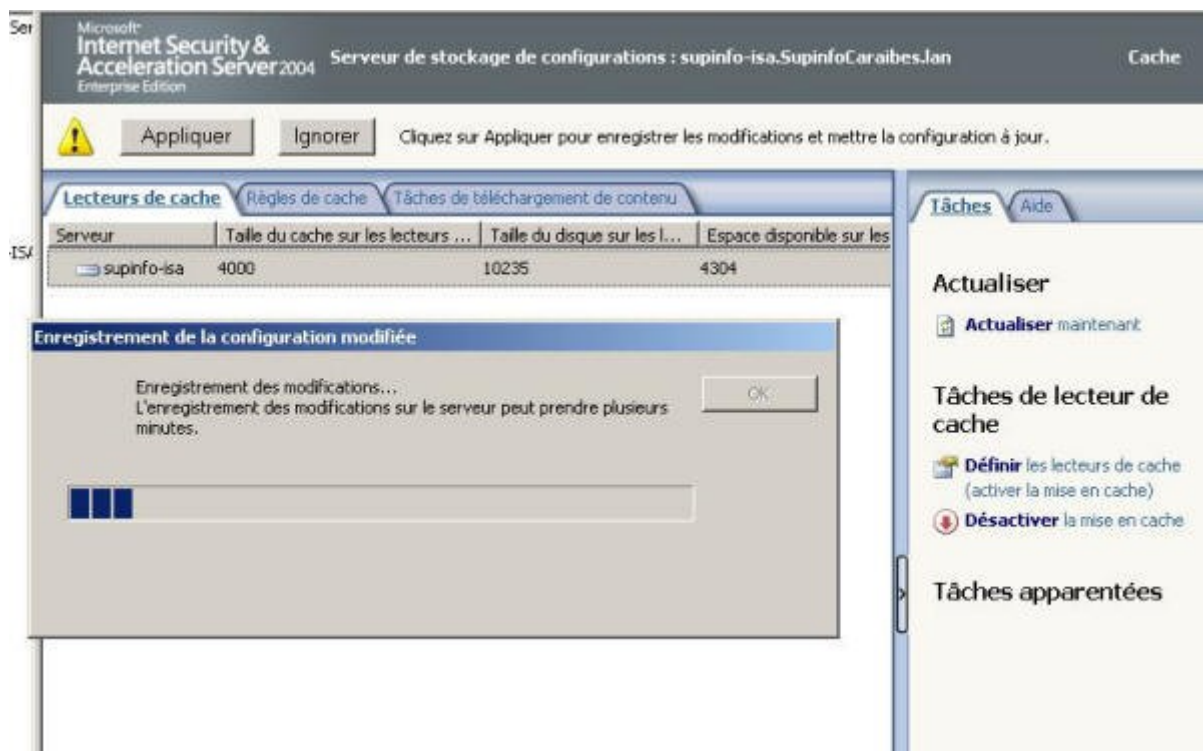
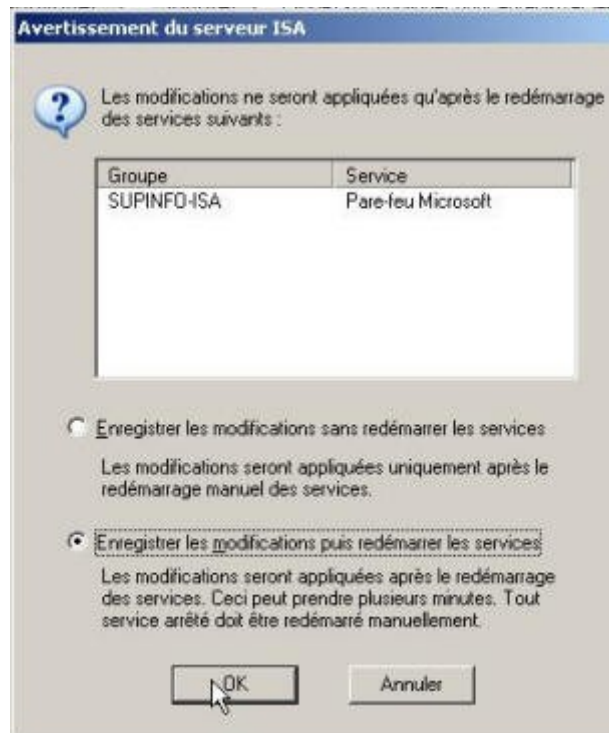


### 5.1.3. Appliquer les modifications

Pour que les modifications prennent effet, il faut absolument les appliquer. Cliquez sur **Appliquer**.



La fenêtre d'information « Avertissement du Server ISA » s'ouvre. Sélectionner l'option « **Enregistrer les informations puis redémarrez les services** » puis cliquez sur **OK**.



Normalement les services s'arrêtent et redémarrent au bout d'une minute. Après avoir redémarré, vérifiez que les services se sont bien relancés. Dans l'arborescence à gauche de la fenêtre ISA Server 2004, cliquez sur **Surveillance**. Au centre de la fenêtre, sélectionnez l'onglet **Tableau de bord**. Vérifiez que les services sont démarrés.

The screenshot shows the Microsoft Internet Security and Acceleration Server 2004 console. The left-hand tree view shows the configuration structure for 'SUPINFO-ISA'. The main console area displays several panels:

- Tableau de bord:** Alerts, Sessions, Services, Configuration, Rapports, Connectivité, Journalisation.
- Connectivité:** A table showing the status of various services:
 

Type de ...	État
Active Directory	non configuré
Autres	non configuré
DHCP	non configuré
DNS	non configuré
Serveurs publiés	non configuré
Web (Internet)	non configuré
- Services:** A table showing the status of core services:
 

Service	État	Serveurs opérés
Pare-feu	Arrêté	0 sur 1
Planificateur ...	Démarré	1 sur 1
MSDE	Démarré	1 sur 1
- Alertes:** A table showing recent alerts:
 

Demière	Alerte	Gravité	Nouveau
23/06/2005 10:22:19	Le service a dém...	Informations	3
23/06/2005 12:18:46	Arrêt du service	Informations	1
23/06/2005 12:18:54	Erreur de configu...	Avertissement	2
- Sessions:** A table showing session statistics:
 

Serveur	Total	Proxy Web	Client de pare-feu	Secu...
supinfo-isa	0	0	0	0
- Rapports:** A table showing report status:
 

Nom du rapport	État	Date de géné...
- Performances système:** A small bar chart at the bottom.

Services arrêtés

The screenshot shows the Microsoft Internet Security and Acceleration Server 2004 console after the services have been restarted. The left-hand tree view is the same. The main console area displays:

- Tableau de bord:** Alerts, Sessions, Services, Configuration, Rapports, Connectivité, Journalisation.
- Connectivité:** Same as the previous screenshot, all services are 'non configuré'.
- Services:** A table showing the status of core services:
 

Service	État	Serveurs opérés
Pare-feu	Démarré	1 sur 1
Planificateur ...	Démarré	1 sur 1
MSDE	Démarré	1 sur 1
- Alertes:** A table showing recent alerts:
 

Demière	Alerte	Gravité	Nouveau
23/06/2005 12:18:46	Arrêt du service	Informations	1
23/06/2005 12:18:54	Erreur de configu...	Avertissement	2
23/06/2005 12:19:43	Le service a dém...	Informations	4
- Sessions:** A table showing session statistics:
 

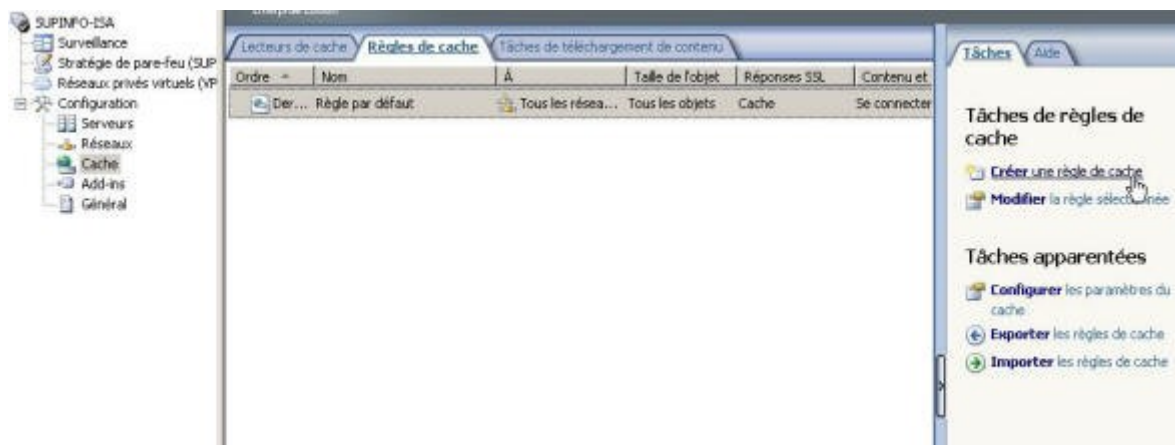
Serveur	Total	Proxy Web	Client de pare-feu	SecureNAT	Client VPN
supinfo-isa	2	0	0	2	0
- Rapports:** Same as the previous screenshot.
- Performances système:** A small bar chart at the bottom.

Services redémarrés

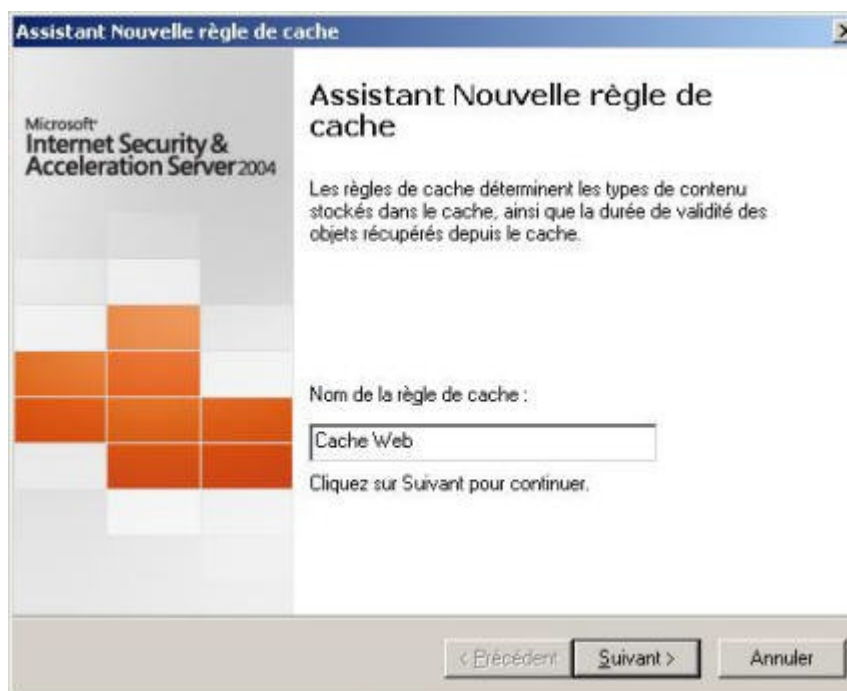


## 5.1.4. Mise en place d'une règle de cache

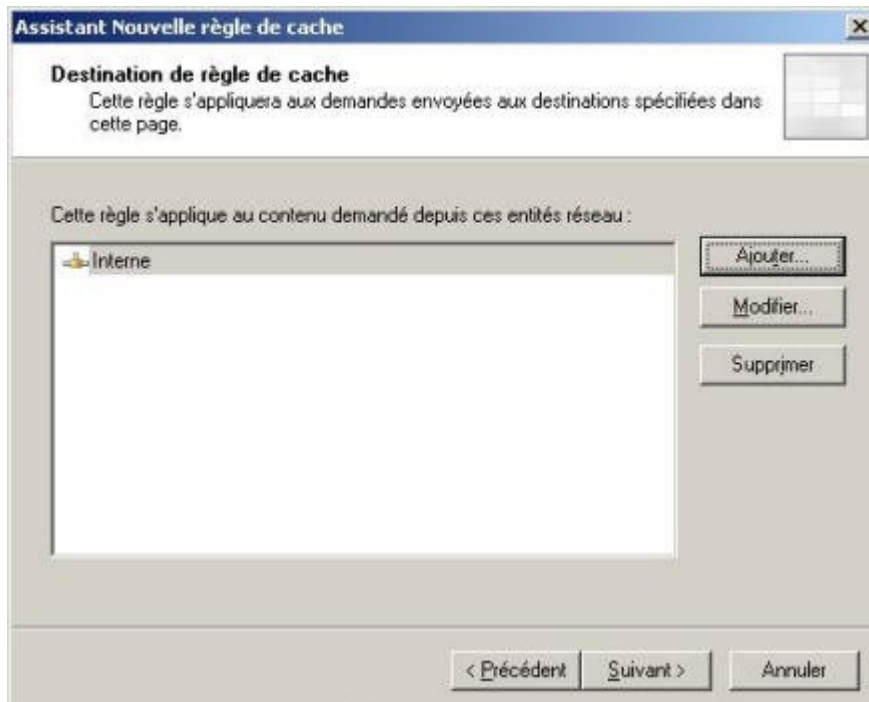
Dans le volet de droite et dans la section « Tâches de règles de cache » cliquez sur **Créer une règle de cache**.



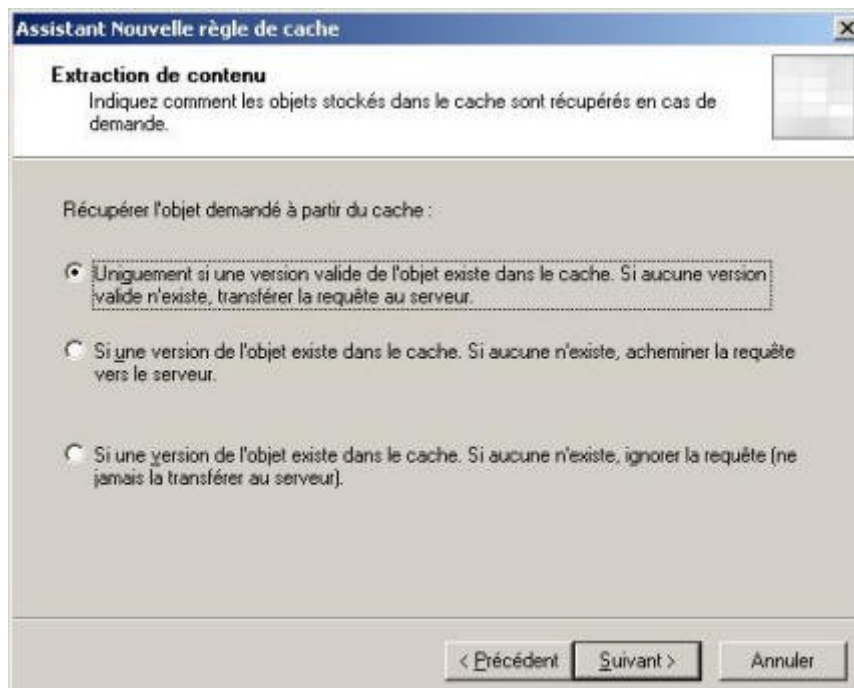
Un assistant se lance et vous demande de nommer la règle. Donnez-lui un nom explicite et cliquez sur **Suivant**.



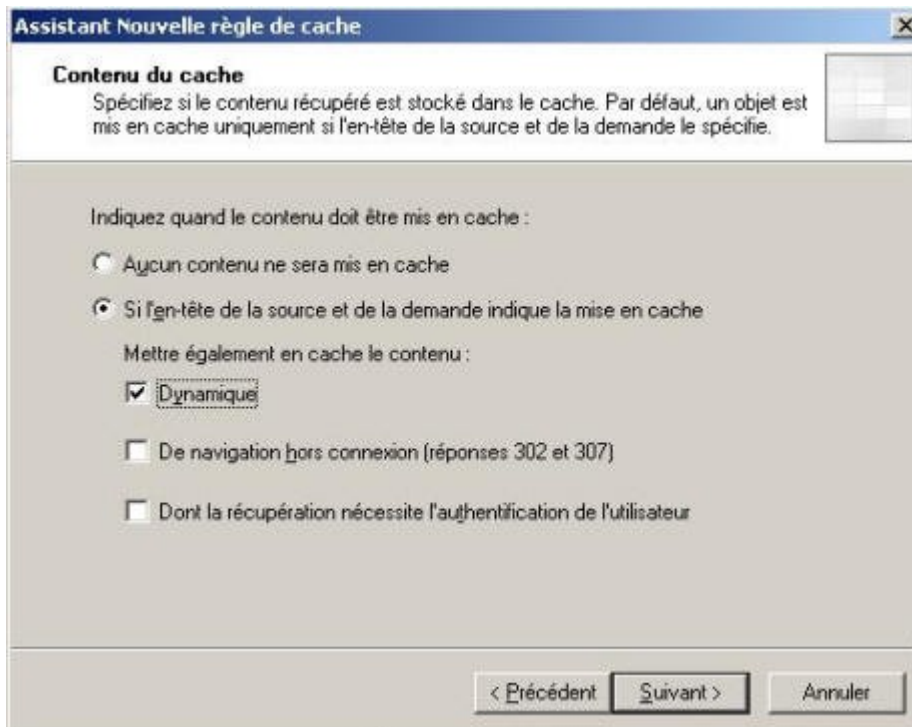
Choisissez les destinations pour lesquelles s'appliquera la règle. Cliquez sur **Ajouter**. Dans la fenêtre des entités réseaux sélectionnez **Interne** et cliquez sur **Ajouter**, puis sur **Fermer**. Validez les destinations en cliquant sur **Suivant**.



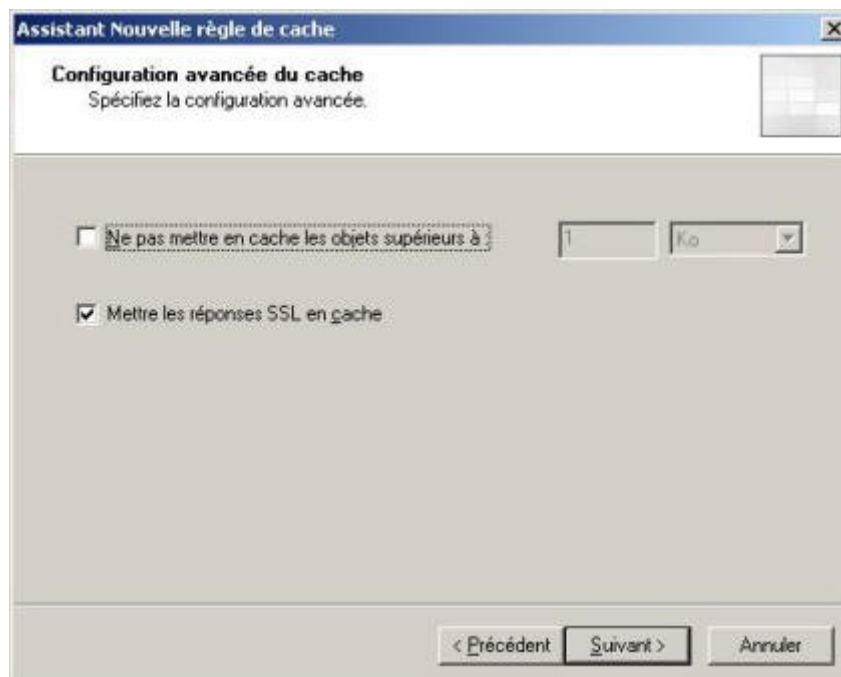
Maintenant indiquez comment les objets stockés dans le cache sont récupérés lors d'une demande. Choisissez **Uniquement si une version valide de l'objet existe dans le cache.** .... Validez le choix en cliquant sur **Suivant**.



Maintenant indiquez comment le contenu récupéré est stockés dans le cache lors d'une demande. Choisissez **Si l'en-tête de la source et de la demande indique la mise en cache.** Cochez également **Mettre en cache le contenu Dynamique.** Validez en cliquant sur **Suivant**.



Laissez les options par défaut et validez en cliquant sur **Suivant**.



Pour les options de mise en cache HTTP, cochez **Activer la mise en cache HTTP** et laissez les options par défaut. Validez en cliquant sur **Suivant**.



**Assistant Nouvelle règle de cache**

**Mise en cache HTTP**  
Lorsque le cache HTTP est activé, les objets HTTP sont stockés dans le cache, comme spécifié par la stratégie.

Activer la mise en cache HTTP

Sauf expiration spécifiée par la source, mettre à jour les objets du cache en fonction de la durée de vie :

Définir la durée de vie des objets (% de l'âge du contenu) :

L'âge du contenu est le temps écoulé depuis la création ou la modification d'un objet.

Limites de durée de vie :

Pas moins de :  Minutes

Pas plus de :  Jours

Appliquer également ces limites de durée de vie aux sources qui spécifient une expiration

La durée de vie est la durée pendant laquelle le contenu du cache est valide, avant qu'il n'expire.

< Précédent   Suivant >   Annuler

Activer le cache FTP puis Validez en cliquant sur **Suivant**.

**Assistant Nouvelle règle de cache**

**Mise en cache FTP**  
Lorsque le cache FTP est activé, les objets FTP sont stockés dans le cache, comme spécifié par la stratégie.

Activer la mise en cache FTP

Durée de vie pour les objets FTP :

Jours

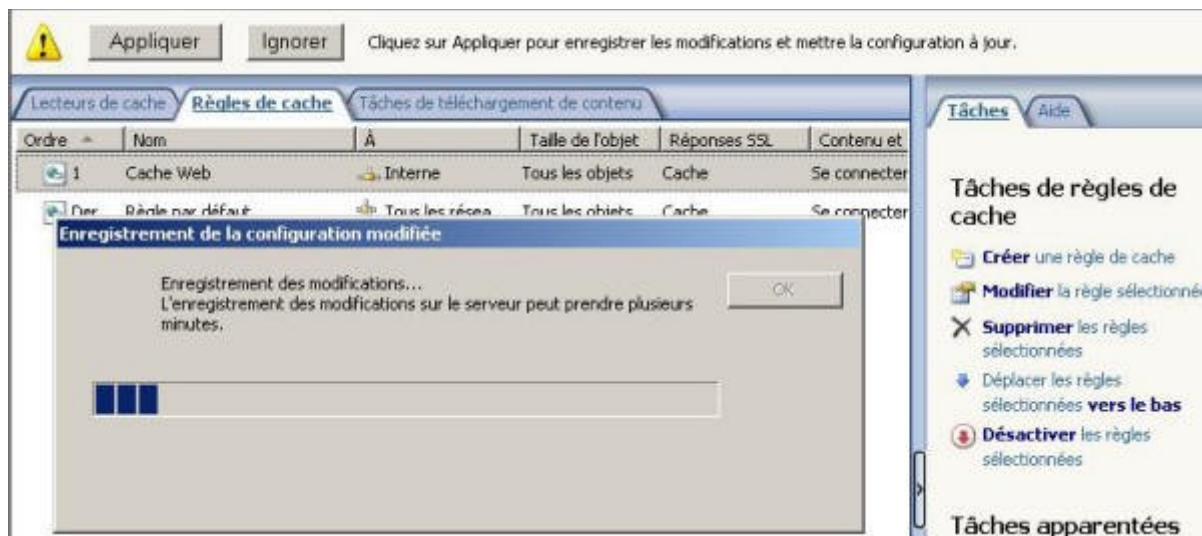
La durée de vie est la durée pendant laquelle le contenu du cache est valide, avant qu'il n'expire.

< Précédent   Suivant >   Annuler

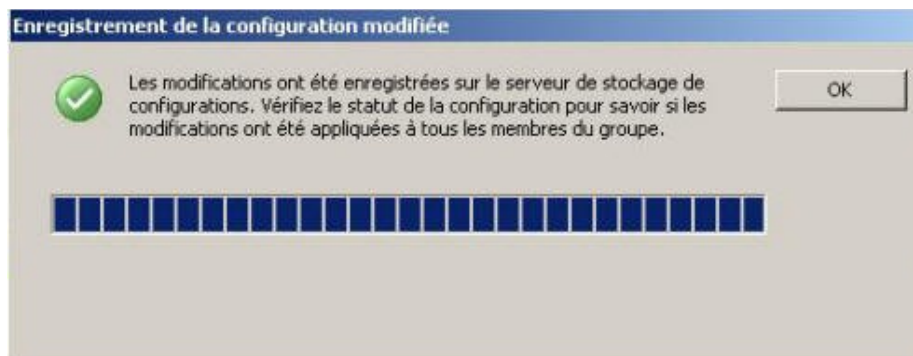
A l'écran récapitulatif cliquez sur **Terminer**. La règle est maintenant créée.



Pour que les modifications prennent effet, il faut absolument les appliquer. Cliquez sur **Appliquer** au dessus des différentes règles.



Une fois les modifications enregistrées, cliquez sur **OK**.

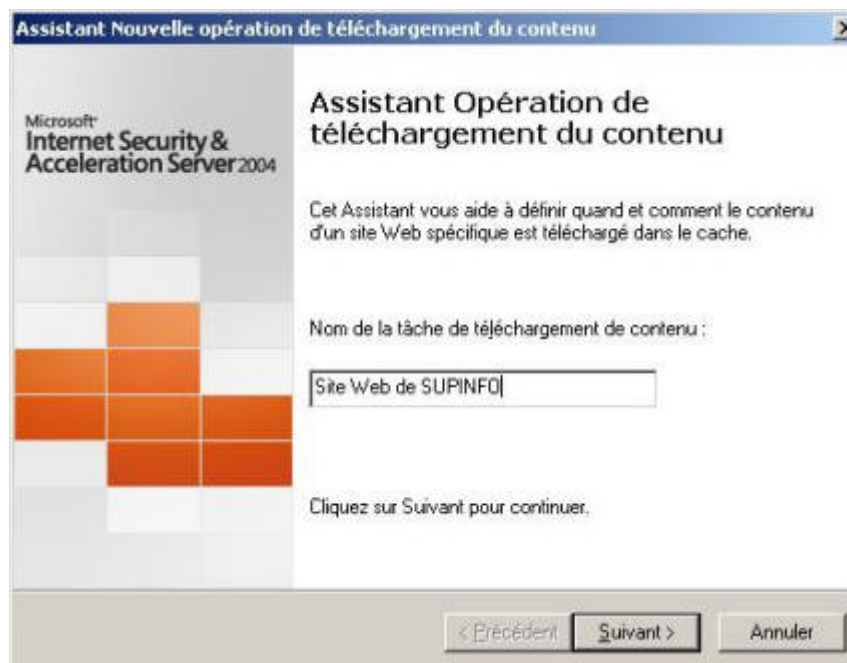


## 5.1.5. Création d'une tâche de téléchargement de contenu

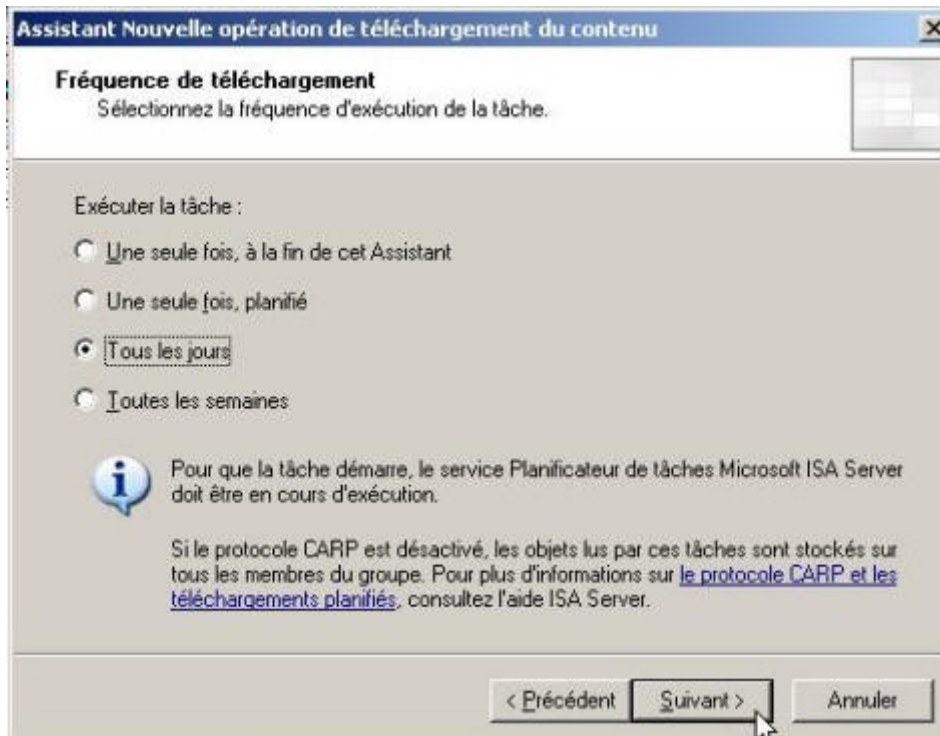
Dans le volet de droite et dans la section « Tâches de téléchargement de contenu » cliquez sur **Planifier une règle de téléchargement de contenu**.



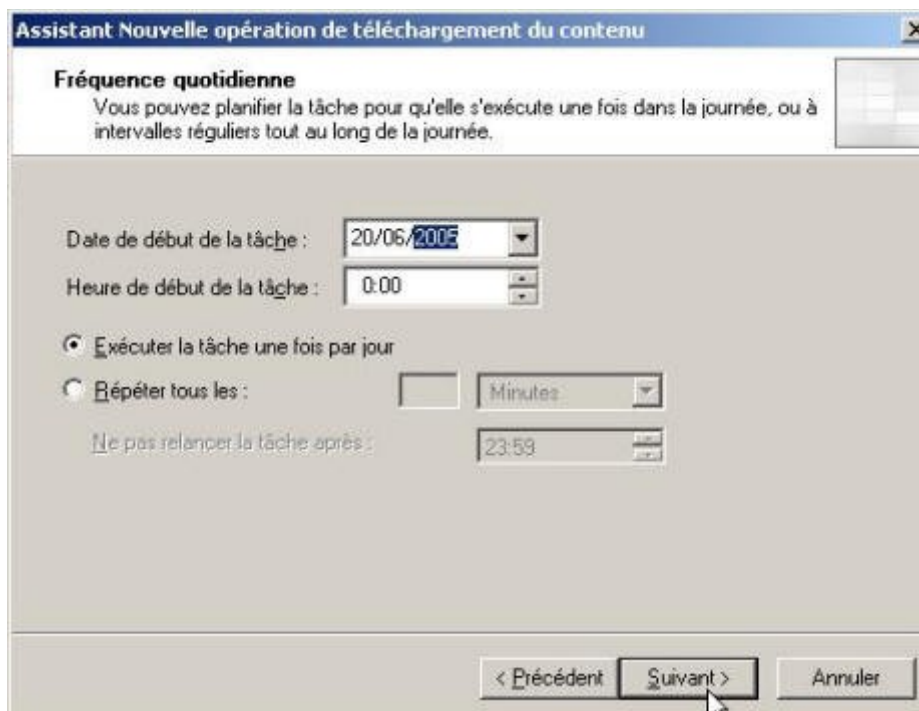
Un assistant se lance et vous demande de nommer la règle. Donnez-lui un nom explicite et cliquez sur **Suivant**.



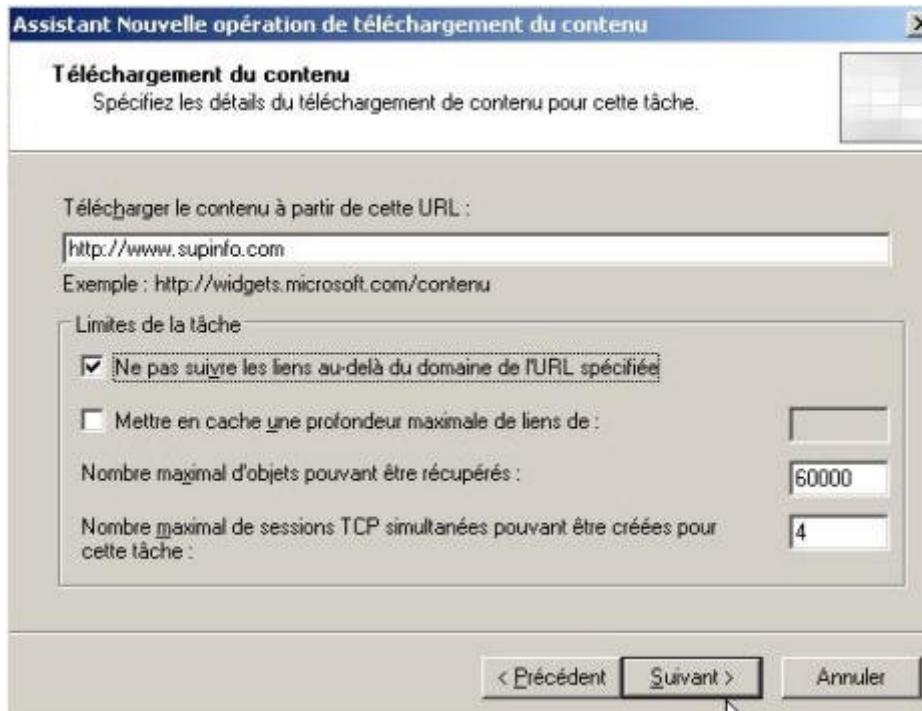
Choisissez la fréquence d'exécution de la tâche de téléchargement puis cliquez sur **Suivant**.



Déterminer la date à partir de laquelle débutera la tâche de téléchargement ainsi que l'heure puis la fréquence de répétition et cliquez sur **Suivant**.



Spécifiez l'URL à partir de laquelle sera téléchargé le contenu ainsi que les limites de la tâche de téléchargement et cliquez sur **Suivant**.



Déterminez les conditions de téléchargement du contenu à mettre en cache et la durée de vie du contenu puis cliquez sur **Suivant**.



A l'écran récapitulatif cliquez sur **Terminer**. La règle est maintenant créée.





Voilà, vous savez maintenant comment activer la mise en cache ainsi que créer une règle de cache et une tâche de téléchargement de contenu de cache.

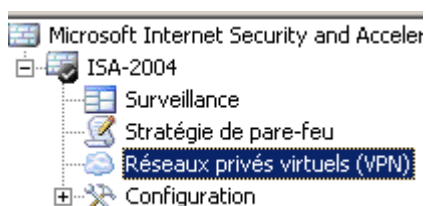
# 6. Mise en place d'un serveur VPN

## 6.1 Introduction

Avec ISA Server 2000, il est possible de mettre en place un **serveur VPN** directement dans la console de gestion ISA. Cependant ce même serveur doit être paramétré comme un serveur VPN « classique » c'est-à-dire dans la console « routage et accès distant ». Avec l'introduction d'ISA Server 2004, on doit réaliser **l'intégralité de la configuration du serveur VPN dans la console de gestion ISA**.

Comme nous allons le voir dans la suite de ce chapitre, cette nouveauté permet une configuration plus aisée et surtout bien plus sécurisée.

## 6.2 Un paramétrage simplifié



Pour commencer, la fenêtre de paramétrage des **réseaux privés virtuels** peut être accédée directement à partir de l'arborescence de la console du serveur ISA.

Cette fenêtre va permettre de mettre en place un serveur VPN en quelques clics. En effet, lorsque l'on sélectionne une topologie réseau avec l'**assistant de configuration réseau**, les paramètres du VPN sont automatiquement réglés pour une **mise en production rapide**.

Ainsi lorsque l'on a choisi la topologie réseau *pare-feu de périmètre*, un serveur VPN est configuré afin d'écouter les éventuelles requêtes faites sur la carte réseau externe en utilisant le **protocole PPTP** (*Point-to-point tunneling protocol*) et la méthode d'authentification **MS-CHAP V2.0** (Microsoft Challenge Handshake Authentication Protocol). De plus le serveur VPN assigne les adresses IP aux clients VPN en utilisant un serveur DHCP et accepte un maximum de 5 connexions.

En résumé, pour rendre le serveur VPN fonctionnel lorsque l'on a choisi la topologie réseau *pare-feu de périmètre*, il faut simplement **activer le serveur VPN** (qui est paramétré automatiquement, mais pas activé) et choisir les groupes et/ou les utilisateurs qui ont le droit de se connecter à distance. On peut donc utiliser le serveur VPN intégré à ISA en trois clics de souris.

Bien entendu, les options du serveur VPN peuvent être modifiées à loisir. Pour cela il faut utiliser l'onglet **Tâches** qui apparaît sur la fenêtre de configuration du VPN. Nous allons voir que le serveur VPN d'ISA possède des fonctions non implémentées dans celui intégré à Windows Server 2003.

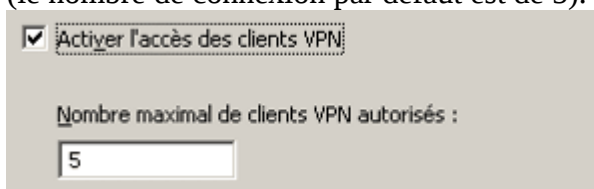


## 6.3 De nouvelles options

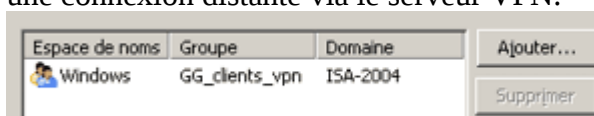
Le menu **Tâches**, ci-contre, permet de paramétrer toutes les options du serveur VPN. L'option *Configurer l'accès des clients VPN* lance une fenêtre composée de quatre onglets :



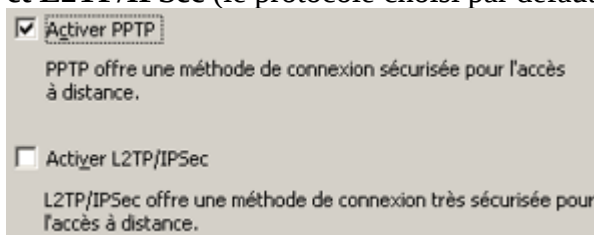
- **Général** : activer/désactiver l'accès des clients au serveur VPN et sélectionner le nombre de connexions simultanées (le nombre de connexion par défaut est de 5).



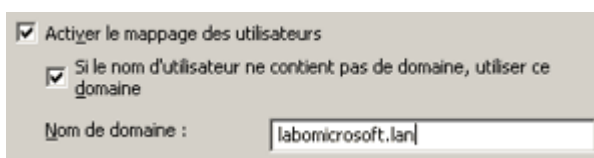
- **Groupes** : choisir les groupes qui ont l'autorisation d'établir une connexion distante via le serveur VPN.



- **Protocoles** : permet de choisir le protocole de tunnelling que l'on souhaite utiliser. Les choix disponibles sont **PPTP** et **L2TP/IPSec** (le protocole choisi par défaut est PPTP).



- **Mappage des utilisateurs** : permet d'appliquer les règles de stratégie d'accès au pare-feu définies par défaut aux clients VPN qui s'authentifient avec **un protocole d'authentification non Windows** (par exemple avec le protocole RADIUS ou le protocole EAP).



Les quatre options situées dans *Configuration VPN générale* (*Sélectionnez les réseaux*, *Sélectionnez les attributions d'adresses*, *Sélectionnez les méthodes d'authentification* et *Spécifier la configuration RADIUS*) renvoient toutes à la même fenêtre qui se compose logiquement de quatre onglets.

---

L2TP : Layer 2 tunneling Protocol (processus d'encapsulation permettant une connexion point-à-point).

IPSec : *Internet Protocol Security* (ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP).

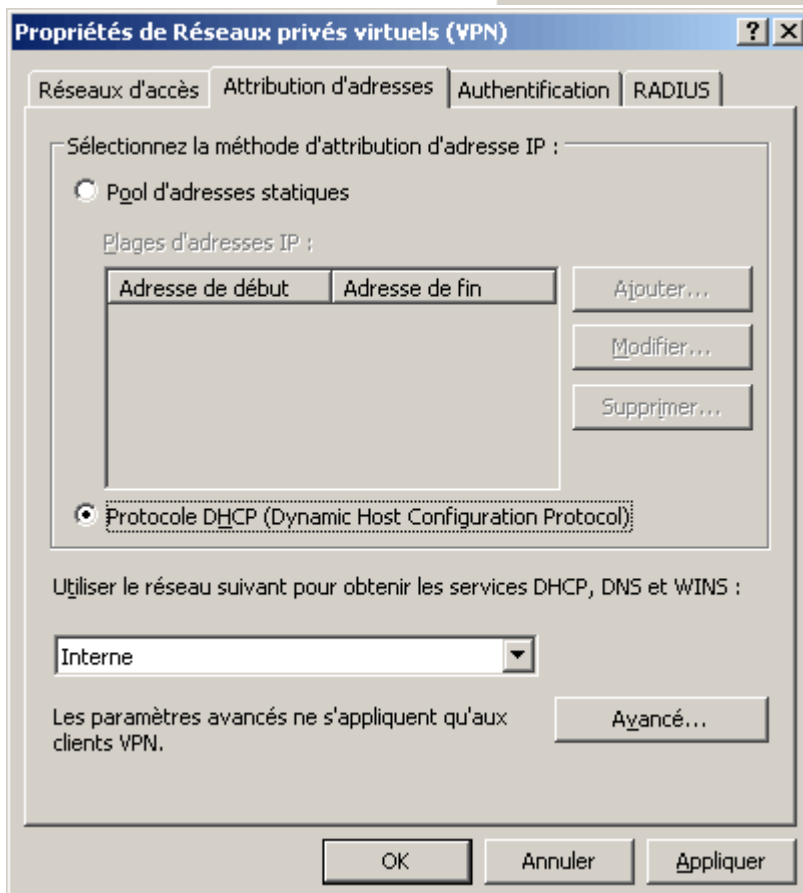
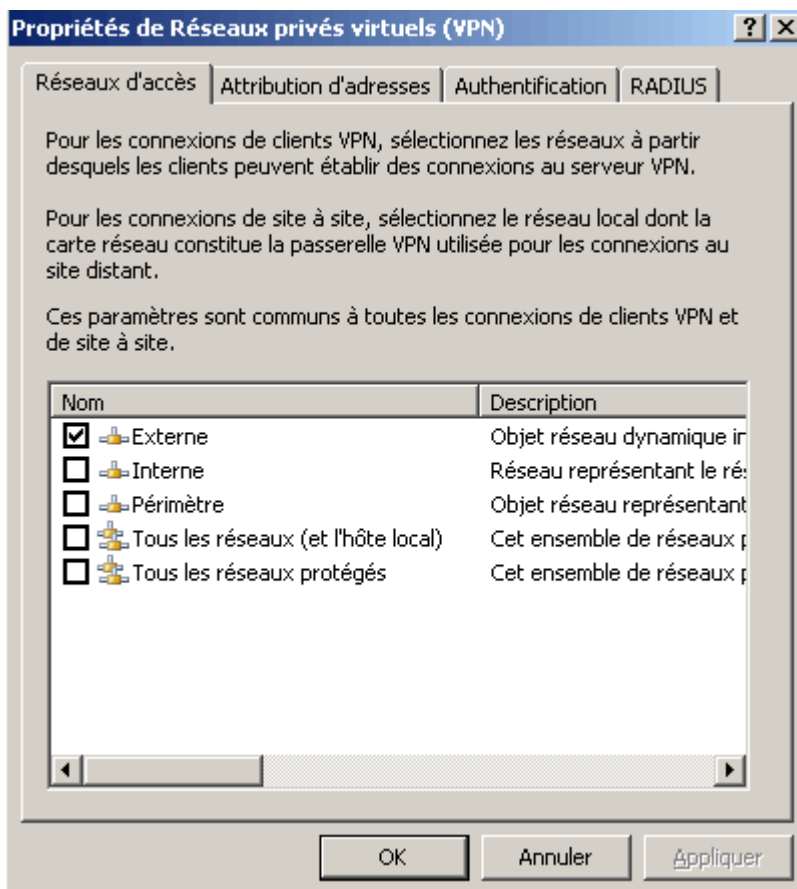
**RADIUS** : *Remote Authentication Dial-In User Service*

EAP : *Extensible Authentication Protocol*

Le premier onglet nommé **Réseaux d'accès** (accessible en cliquant sur *Sélectionnez les réseaux d'accès*) permet de choisir à partir de **quelle interface** le serveur VPN sera accessible par les clients et/ou les autres serveurs VPN.

Dans le cas du pare-feu de périmètre, le paramètre par défaut est le **réseau externe**.

Cela est normal puisque avec cette topologie, on possède deux réseaux : un **réseau interne** (le réseau privé de l'entreprise) et un **réseau public** (Internet). On souhaite bien entendu faire bénéficier les clients externes de l'accès à distance et non l'inverse.



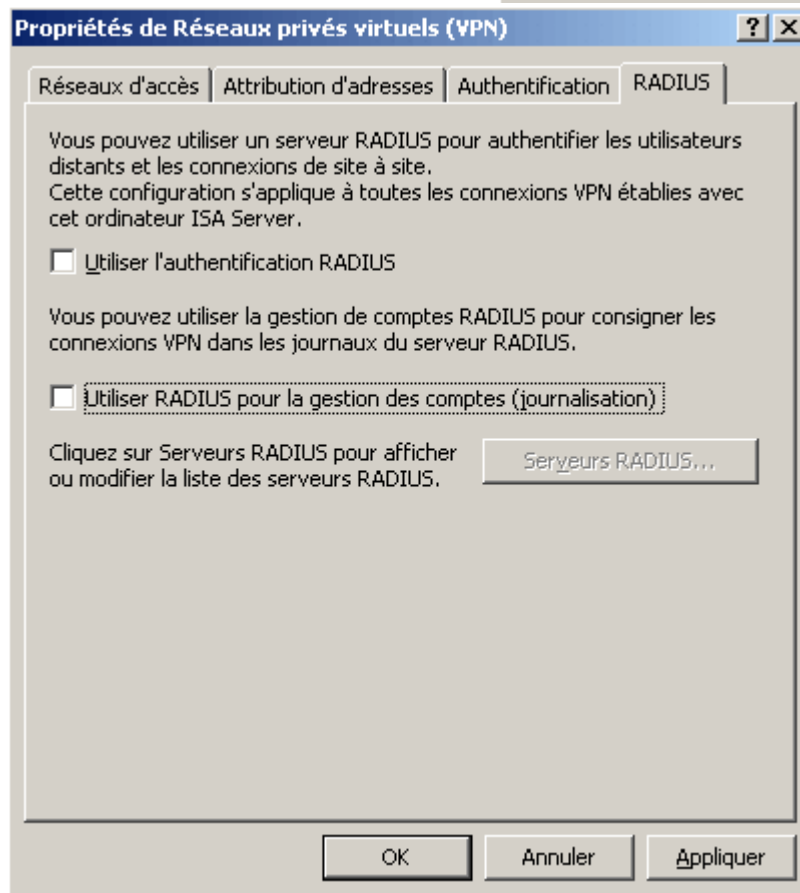
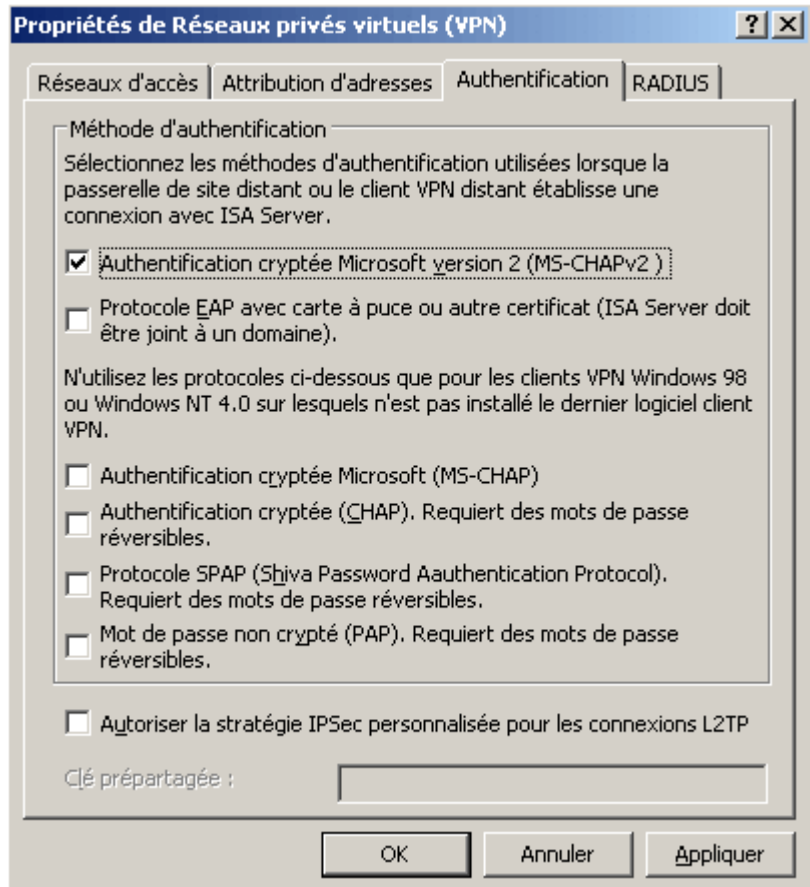
L'onglet **Attribution d'adresses** (accessible en cliquant sur *Définir les attributions d'adresses*) permet de forcer le serveur VPN à assigner lui-même les adresses IP aux clients VPN parmi une plage d'adresses prédéfinies ou bien à utiliser les adresses fournies par un serveur DHCP.

Dans le second cas, on doit sélectionner l'interface sur laquelle le serveur VPN essaiera de contacter **un serveur DHCP** et choisir (en cliquant sur le bouton *Avancé*) si les adresses IP des serveur DNS et WINS seront dynamiques (c'est-à-dire attribuées par le serveur DHCP en même temps que l'adresse IP du client) ou bien statiques.

L'onglet **Authentification** (accessible en cliquant sur *Sélectionnez les méthodes d'authentification*) propose un large choix de protocoles pour permettre l'authentification des clients d'accès distant.

Le protocole sélectionné par défaut est **MS-CHAP v2**. On peut aussi utiliser **EAP**. D'autres méthodes, moins sécurisées, sont présentes mais uniquement à titre de compatibilité. On peut citer MS-CHAP, CHAP, SPAP et PAP.

Enfin, il est possible d'utiliser une **clé pré partagée** si l'on utilise le **protocole L2TP/IPsec**.



Une des principales nouveautés d'ISA Server 2004 est la possibilité de pouvoir utiliser **un serveur RADIUS** pour authentifier les clients d'accès distants.

L'onglet **RADIUS** (accessible en cliquant sur *Sélectionnez la configuration RADIUS*) propose d'activer cette fonctionnalité. Dans le cas où ce paramètre est sélectionné on peut choisir d'enregistrer les événements liés à l'établissement et à la fermeture des sessions VPN dans le journal du serveur RADIUS.

Pour spécifier la liste de serveurs RADIUS à contacter il faut cliquer sur le bouton *Serveurs RADIUS* et entrer les serveurs dans l'**ordre de priorité** avec lequel ils doivent être utilisés.

---

**WINS** : *Windows Internet Naming Service*

## 6.4 La fonction de mise en quarantaine

Une des fonctionnalités les plus innovantes d'ISA Server 2004 reste **la mise en quarantaine** des clients VPN. En effet, la mise en place d'un serveur VPN pose un gros problème en ce qui concerne la sécurité malgré le fait que le processus d'authentification et que les échanges soient cryptés. La faille provient souvent des machines clientes car **elles sont souvent infectées par divers virus, vers, chevaux de Troie et autres logiciels espions**. Ces virus, par le biais du réseau privé virtuel, finissent par se retrouver sur le réseau de l'entreprise, **ruinant ainsi tous les efforts des administrateurs réseau !**

La fonction de mise en quarantaine permet d'**isoler les clients ne répondant à certains critères dans un réseau spécifique** nommé **clients VPN en quarantaine**. Les critères de sélections doivent être définis dans un script qui s'exécute après l'authentification des clients. **Ce script n'est pas fourni par Microsoft** avec ISA Server et doit donc être développé par l'administrateur ce qui offre une plus grande flexibilité. Il est tout de même dommage que Microsoft ne se soit pas donné la peine de fournir des scripts prédéfinis pour certains scénarios. On peut notamment créer un script vérifiant si le pare-feu du client est actif et si son antivirus et son système sont à jour.

# 7. Configuration des ordinateurs clients

## 7.1 Introduction

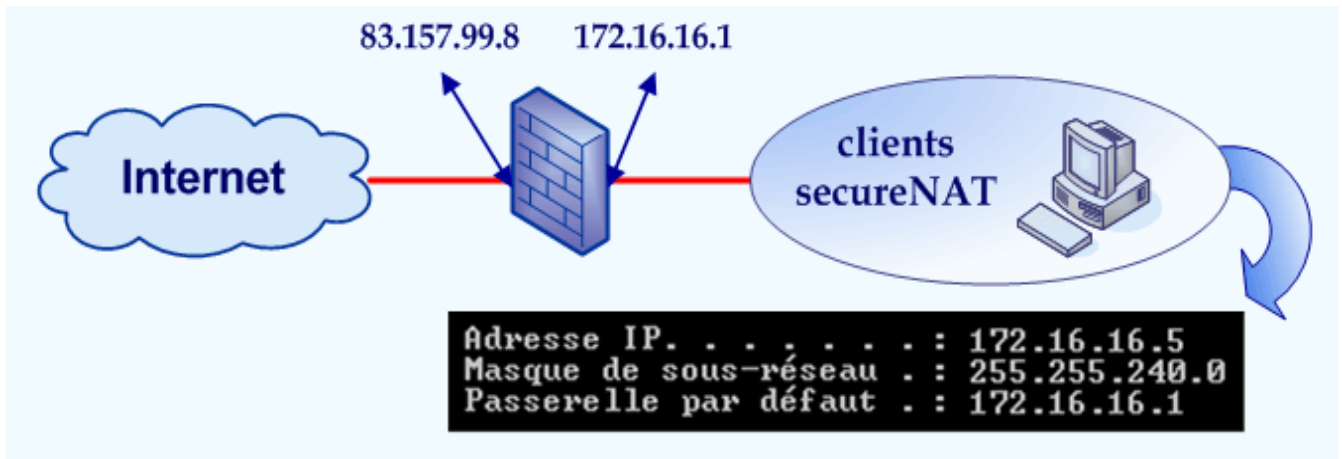
Il est possible de configurer les ordinateurs clients de trois manières différentes. C'est pourquoi on en distingue **trois types** :

- les **clients de pare-feu**
- les **clients du Proxy web**
- les **clients SecureNAT**

Les possibilités offertes en terme de **sécurité**, de **fonctionnalités** mais aussi de **déploiement** diffèrent en fonction du type de client.

## 7.2 Configurer un client SecureNAT

Un client SecureNAT est un ordinateur configuré pour utiliser l'adresse IP du serveur ISA en tant que **passerelle par défaut**. Toute machine exécutant un système d'exploitation sur lequel la **pile de protocole TCP/IP** est supportée (UNIX, BSD, Linux, Windows,...) peut donc devenir un client SecureNAT. Bien évidemment lorsqu'un ou plusieurs routeurs séparent le client SecureNAT du serveur ISA, le client devra utiliser l'adresse IP du routeur le plus proche de lui en tant que passerelle par défaut. Ce type de client s'avère **simple et rapide à implémenter** lorsque le protocole DHCP est utilisé (en effet, il n'y a qu'une option à paramétrer au niveau du serveur DHCP pour que les clients SecureNAT fonctionnent).



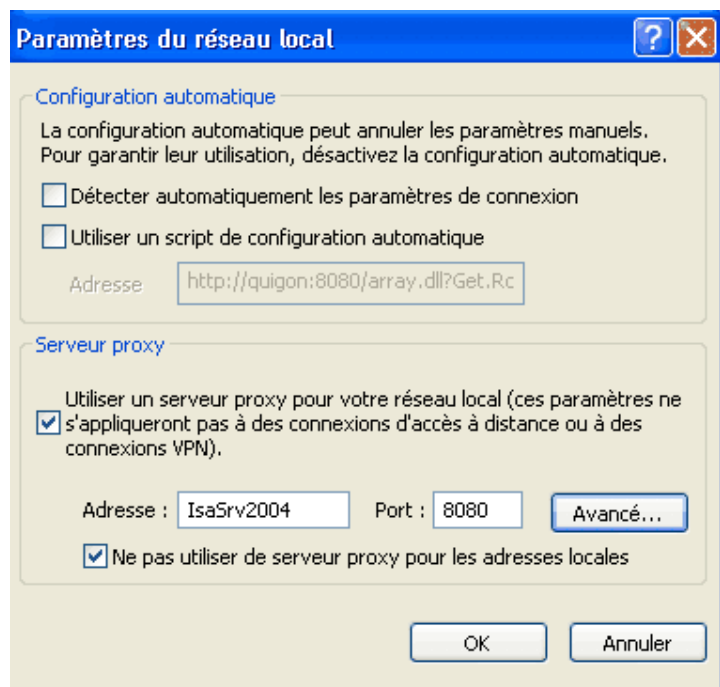
L'un des défauts majeur du client SecureNAT est l'absence de système d'authentification. En effet, là où le client de pare-feu et le client du Proxy web permettent de retrouver l'identité de l'utilisateur, le client SecureNAT permet uniquement de retrouver l'adresse IP de la machine. Cela signifie que les restrictions sur les utilisateurs et les groupes d'utilisateurs ne s'appliquent pas aux clients SecureNAT. Ceci explique pourquoi ils sont utilisés uniquement lorsque cela est nécessaire :

- dans le cas d'**ordinateurs ne supportant pas le client pare-feu** (c'est-à-dire sous Unix/Linux)
- dans le cas de **serveurs devant être publiés**

### 7.3 Configurer un client du Proxy web

Un client du Proxy web est un ordinateur exécutant **une application configurée pour utiliser le serveur ISA en tant que serveur de proxy**. L'exemple type est un **navigateur web** comme Safari, Opéra ou bien encore Internet Explorer. Voici quelques caractéristiques des clients du Proxy web :

- ils sont utilisables sur **n'importe quel système d'exploitation** (sauf les OS ne gérant pas TCP/IP et ne possédant aucun navigateur web...).
- les seuls protocoles supportés sont **HTTP, HTTPS et FTP sur HTTP** (protocole permettant de consulter le contenu d'un serveur FTP à l'aide d'un navigateur web en saisissant des adresses du type [ftp://nom\\_du\\_serveur](ftp://nom_du_serveur) dans la barre des URL).
- Ils proposent **d'authentifier ou non les utilisateurs**.

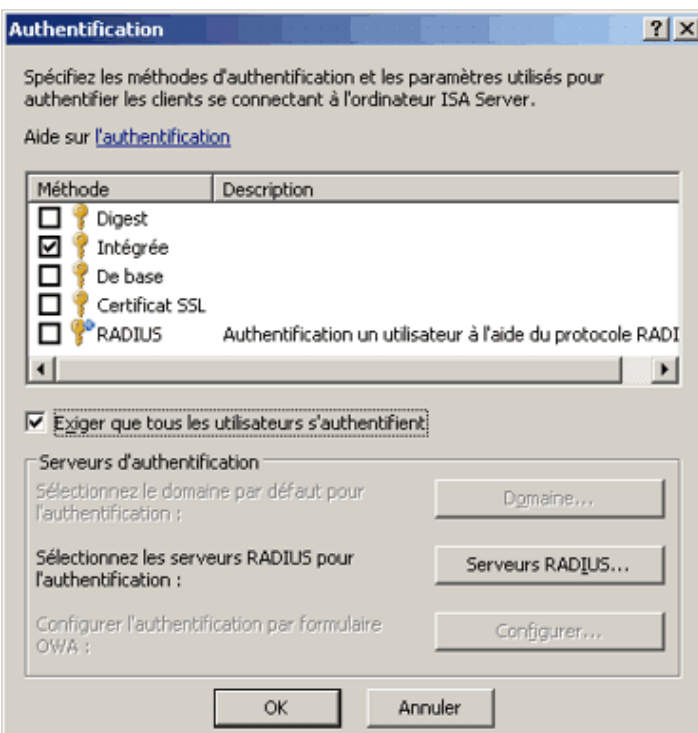
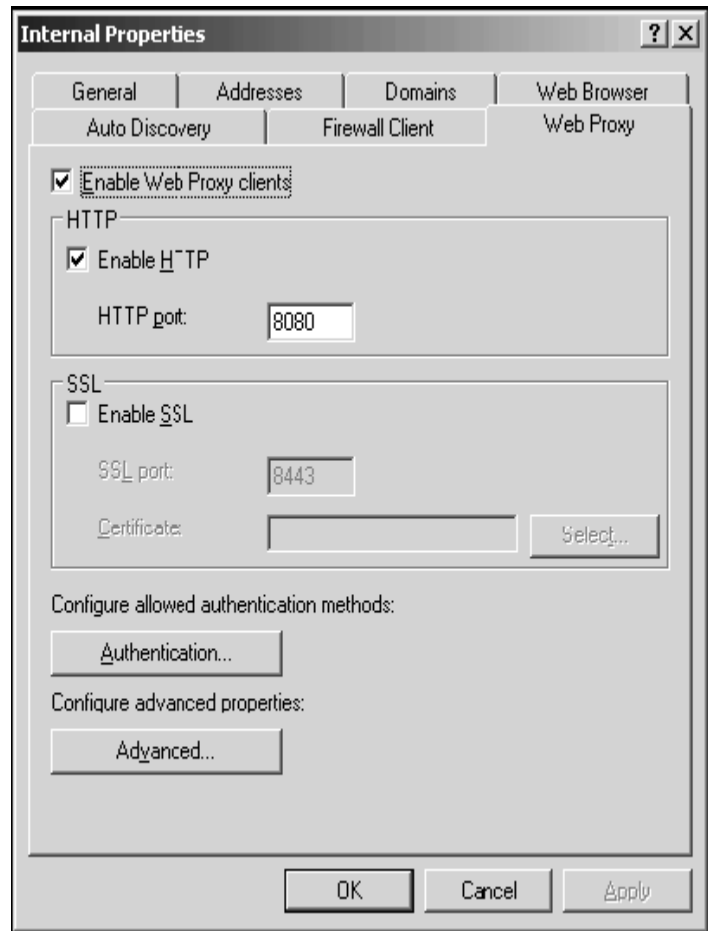


La figure précédente montre la capture d'écran d'un ordinateur exécutant Internet Explorer et configuré en tant que client du Proxy web. **Il suffit définir le nom du serveur ISA ainsi que le**

**port utilisé** dans le navigateur (cette fenêtre est accessible via *Outils / Options Internet / Connexions / Paramètres réseaux*). Bien entendu, l'apparence et l'emplacement de ces paramètres changent d'un logiciel à l'autre.

Lorsque le serveur ISA reçoit une requête sur le port 80, le client est toujours considéré comme un client du Proxy web, et ce quelque soit sa configuration réelle (SecureNAT, Proxy web ou pare-feu).

Par défaut, **ISA Server 2004 utilise le port 8080** pour communiquer avec les clients du Proxy web. Pour modifier ce paramètre, il faut afficher les **propriétés du réseau Interne** en développant *Configuration / Réseaux* dans l'arborescence de la console de Gestion ISA. L'onglet **Proxy web** permet de modifier les ports utilisés pour les protocoles HTTP et HTTPS (les valeurs par défaut sont respectivement 8080 et 8443).



protocole réellement utilisé est **WDigest**.

- **Intégrée** : L'authentification dite Intégrée correspond au protocole **Kerberos V5** (ou NTLM dans certains cas). Kerberos met en oeuvre le **hachage des données** et propose une **authentification mutuelle**.
- **Certificat SSL** : Cette méthode vérifie l'identité du client et du serveur à l'aide de **certificat numériques** préalablement distribués par une autorité de certification. Le protocole de cryptage utilisé est **SSL pour Secure Sockets Layer**.
- **RADIUS** : RADIUS signifie **Remote Authentication Dial-In User Service**. C'est un protocole d'authentification standard faisant intervenir le protocole de **hachage MD5**.

NTLM : *NT Lan Manager*

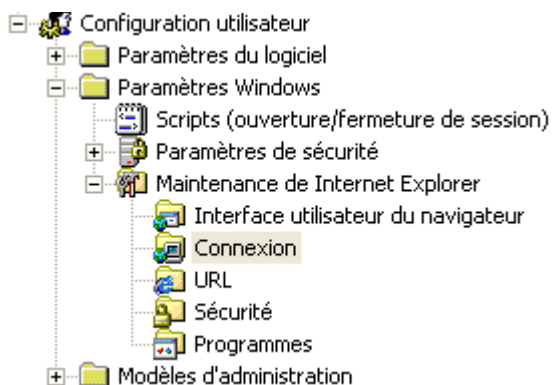
La méthode d'authentification à privilégier au sein d'un domaine reste l'**authentification intégrée à Windows** en raison de son haut niveau de sécurité. La mise en place de l'authentification des clients du Proxy web ne doit pas être négligée sinon les restrictions des règles d'accès sur les utilisateurs et sur les groupes d'utilisateurs ne s'appliqueront pas. En outre, l'authentification permet d'**obtenir des statistiques concernant les utilisateurs par le biais des rapports**.

Dès que l'une des méthodes d'authentification a été choisie, une fenêtre équivalente à celle présentée ci à droite apparaît. Deux possibilités s'offrent à l'utilisateur :

- Renseigner les champs **Nom d'utilisateur** et **Mot de passe** à chaque nouvelle instance du navigateur
- **Mémoriser** l'identifiant et le mot de passe pour ne plus avoir à les remplir



#### **7.4 Utilisation du protocole WPAD pour paramétrer automatiquement les clients du Proxy web(Web Proxy AutoDetect)**

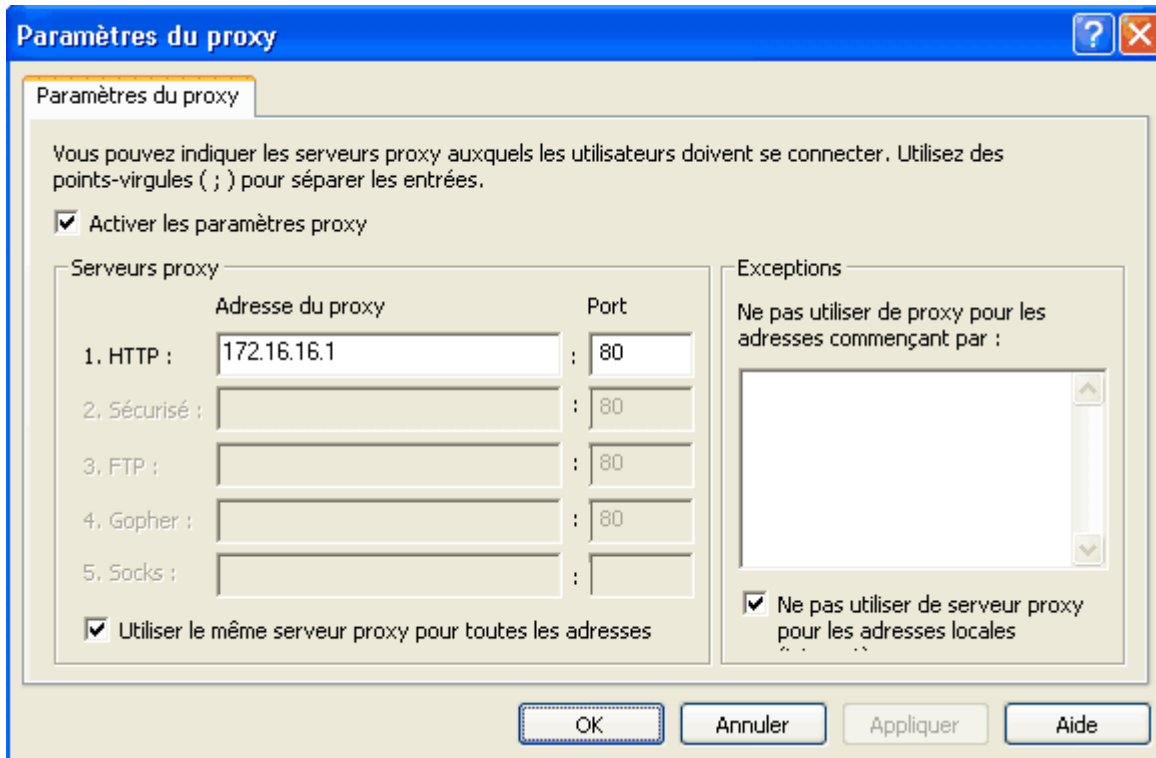


Lorsque les ordinateurs utilisent **Microsoft Internet Explorer**, leur configuration en tant que clients du Proxy web est facilitée. En effet, il est possible de configurer les paramètres du Proxy à l'aide d'un objet **stratégie de groupe ou GPO** (Group Policy Object). Cela implique évidemment que les ordinateurs appartiennent à un **domaine Active Directory**.

Les paramètres du Proxy (adresse IP, port, ...) pour Internet Explorer sont configurables au niveau du **compte d'utilisateur** ou bien au niveau du **compte d'ordinateur**. Dans les deux cas, il faut développer *Paramètres Windows / Maintenance de Internet Explorer / Connexion* à l'aide de la console **Éditeur**



## de stratégie de groupe.



Lorsqu'une application autre que Internet Explorer doit être configurée, la tâche se révèle plus contraignante puisqu'il n'existe aucun moyen de l'automatiser. Les clients doivent donc être configurés manuellement ce qui entraîne :

- une **perte de temps lors de la configuration initiale** des applications
- une **perte de temps si le serveur de Proxy change d'adresse IP** (il faut alors reconfigurer à la main toutes les applications alors qu'avec une GPO il n'y a qu'une valeur à modifier une seule fois)
- une **perte de temps si l'ordinateur qui héberge le programme est mobile**. En effet, un cadre se déplaçant de succursale en succursale avec son ordinateur portable devra reconfigurer manuellement l'adresse IP du serveur de Proxy à chaque changement de site (en supposant qu'il y ait un serveur de Proxy par site). Dans ce cas bien précis, une GPO n'est d'aucun secours...

Pour palier à cela, il est possible d'implémenter le **protocole WPAD** (Web Proxy AutoDetect) qui permet de **configurer automatiquement les programmes pour pointer vers le bon serveur de proxy**. Bien entendu les applications doivent être conçues pour **supporter WPAD** (tous les navigateurs récent tels Opéra, IE, Safari, Konqueror, Firefox ou bien encore Netscape Navigator le supportent). C'est par exemple le cas avec Internet Explorer depuis la version 5.0 et Netscape Navigator depuis la version 2.0. WPAD propose deux manières différentes pour configurer automatiquement les applications web :

- à l'aide d'un **enregistrement de ressource spécifique dans le serveur DNS**
- à l'aide d'une **option spécifique dans le serveur DHCP**

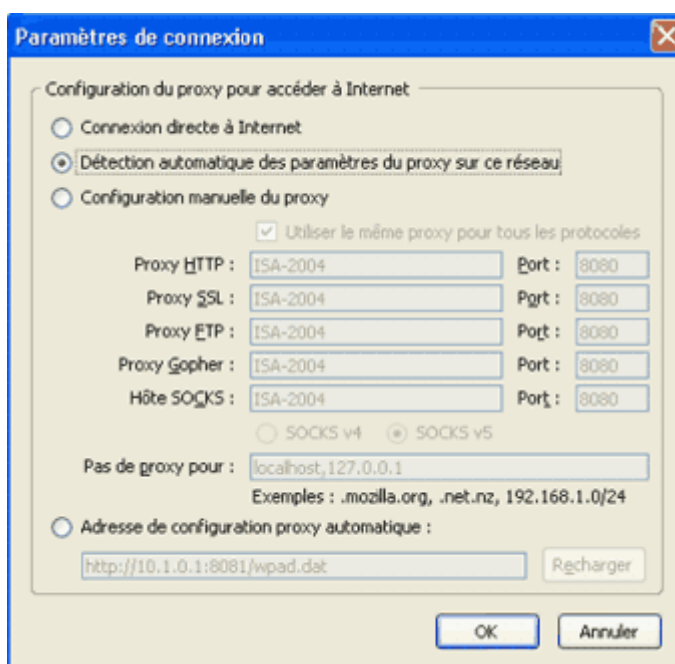
Publier les informations de détection automatique

Utiliser ce port pour les détections automatiques :

La première chose à faire avant même de configurer le serveur DNS ou bien le serveur DHCP est d'**activer la prise en charge du protocole WPAD au niveau du serveur ISA**. Pour cela, il suffit d'aller dans les propriétés du réseau **Interne**, puis de cocher la case **Publier les informations de détection automatique**, située dans l'onglet **Détection automatique**.

Par défaut, les informations de configuration automatique sont **publiées sur le port 80**. Il est possible de modifier cette valeur mais cela n'est pas recommandé. En effet, certains programmes ne peuvent détecter automatiquement la configuration du serveur Proxy que via le port 80. C'est notamment le cas des **navigateurs basés sur le moteur d'affichage Gecko** (Mozilla / Firefox / Netscape Navigator)

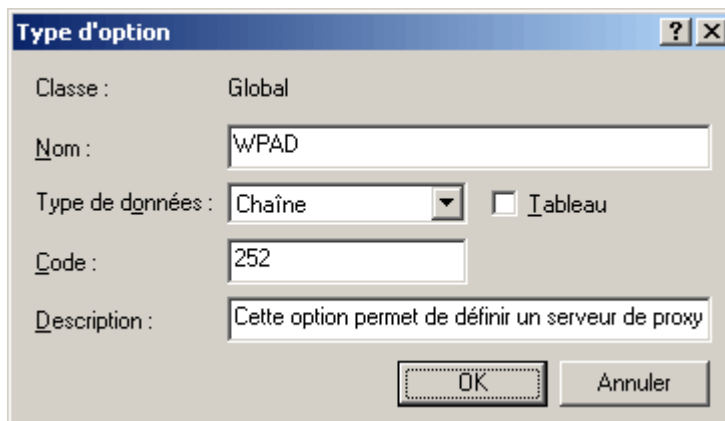
Si vous choisissez d'utiliser un port différent avec ces navigateurs, il faudra spécifier l'adresse de configuration automatique du Proxy manuellement **ce qui s'avère aussi contraignant** que de définir l'adresse du serveur de Proxy de façon classique... **L'utilisation du port 80 est donc de mise pour ce service** sauf si une autre application utilise déjà ce port sur le serveur ISA.



Ci-contre la fenêtre de configuration des paramètres de connexion du navigateur Firefox dans sa version 1.0. On remarque que l'option *Détection automatique des paramètres du Proxy sur ce réseau* a été activée ce qui signifie que Firefox essaye de se configurer automatiquement à l'aide du protocole **WPAD** en effectuant une recherche sur le port 80.

Pour configurer un grand nombre de machines en tant que clients du Proxy web, l'utilisation du **serveur DHCP** se révèle la plus efficace. Pour cela il faut **créer une nouvelle option DHCP** (clic droit sur le nom du serveur, puis *Définir les options prédéfinies...* dans la console DHCP). Ci-contre, la fenêtre de création d'une option DHCP. Il faut définir plusieurs paramètres :

- le **nom** de l'option
- le **type de données** (la case à cocher tableau permet de créer des options multivaluées)
- le **code** de l'option
- une **description** (facultative)



Il faut ensuite attribuer la valeur [http://nom\\_du\\_serveur\\_de\\_proxy:port\\_utilisé/wpad.dat](http://nom_du_serveur_de_proxy:port_utilisé/wpad.dat) à l'option WPAD précédemment créée. Bien entendu, vous pourrez appliquer cette option au niveau du serveur, d'une étendue, d'une classe DHCP ou bien encore d'un client réservé.

Options d'étendue			
Nom d'option	Fabricant	Valeur	Classe
006 Serveurs DNS	Standard	172.16.16.1, 172.16.16.2	Aucun
015 Nom de domaine DNS	Standard	laboms.net	Aucun
044 Serveurs WINS/NBNS	Standard	172.16.16.2	Aucun
046 Type de nœud WINS/NBT	Standard	0x8	Aucun
252 protocole WPAD	Standard	http://isa-2004.laboms.net:80/wpad.dat	Aucun

Nom	Type ▲	Données
WPAD	Alias (CNAME)	isa-2004.laboms.net
isa-2004	Hôte (A)	10.1.0.1

L'administrateur peut aussi utiliser le **serveur DNS** pour configurer automatiquement les ordinateurs clients en tant que clients du Proxy web. Il suffit simplement de créer un enregistrement de ressource de type **Alias (CNAME)** nommé **WPAD** pointant vers le **nom de domaine pleinement qualifié (FQDN)** du serveur de proxy.

Cet enregistrement doit être créé dans le même domaine que les ordinateurs clients. Lorsque l'option DHCP 252 n'a pas été affectée, le client contacte le serveur DNS pour savoir si il existe **un enregistrement de ressource nommé wpad.suffixe\_dns\_client**. Le client récupère donc l'adresse IP du serveur de Proxy en deux étapes :

- le client cherche le FQDN correspondant à **wpad.laboms.net** (le serveur DNS renvoie la réponse isa-2004.laboms.net)
- le client cherche l'adresse IP correspondant à **isa-2004.laboms.net** (le serveur DNS renvoie la réponse 10.1.0.1)

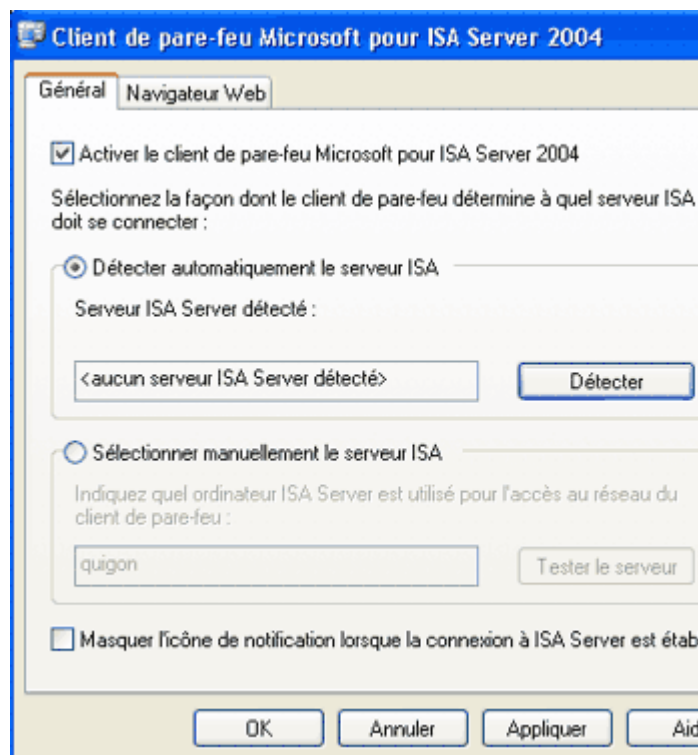
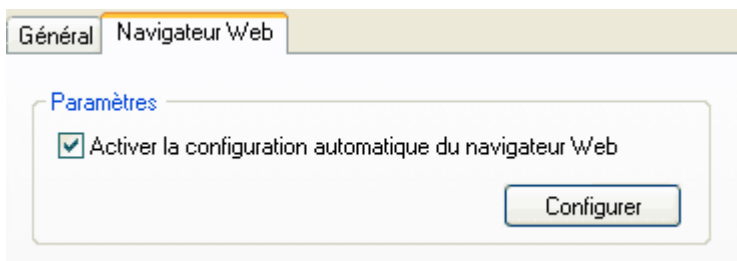
## 7.5 Déploiement et configuration du client pare-feu

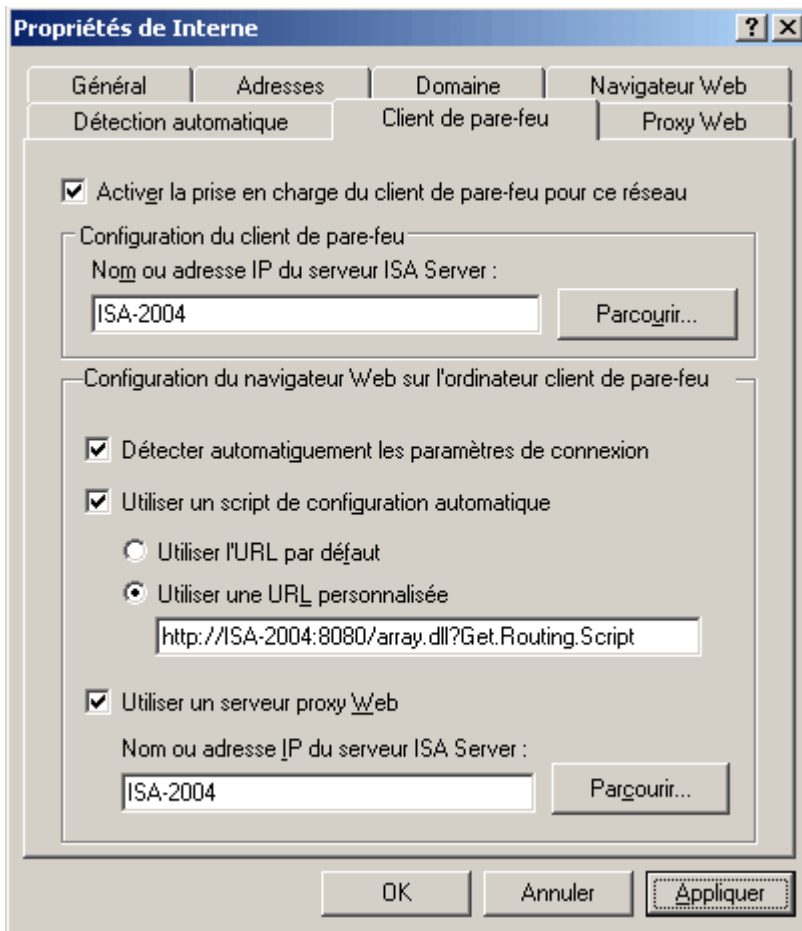
Un **client pare-feu** est un ordinateur sur lequel l'application **client de pare-feu Microsoft** est installée. Cette application configure automatiquement la machine pour accéder à Internet ou à un autre réseau par l'intermédiaire d'un serveur ISA. Il est possible de déployer ce logiciel de diverses manières :

- via le **partage** `\\serveur_isa_2004\mspcnlt` crée automatiquement lors de l'installation d'ISA
- via un **objet stratégie de groupe** (GPO) (par la création d'un paquet de distribution de logiciel).
- via un **package System Management Server** (SMS) 2003 (une solution complète d'administration de parc informatique, d'inventaire, de gestion et déploiement des applications et de mises à jour de sécurité.)

Après l'installation du client pare-feu ; une icône apparaît dans la zone de notification (system tray). Pour configurer le client pare-feu, faite un clic avec le bouton droit puis cliquez sur configurer.

Le paramétrage du client de pare-feu est on ne peut plus simple. L'onglet **Général** permet de sélectionner **manuellement ou automatiquement** le serveur ISA. Dans le second cas, le protocole **WSPAD** (WinSock Proxy AutoDetect) est utilisé. WSPAD se configure de la même manière que WPAD (via un serveur DHCP ou un serveur DNS). L'onglet **Navigateur Web** permet quand à lui de **configurer automatiquement Internet Explorer**. Les paramètres appliqués au navigateur doivent être définis au niveau du serveur ISA.





On peut configurer les **paramètres du Proxy** que va recevoir le navigateur (par l'intermédiaire du logiciel client de pare-feu Microsoft) dans les propriétés du réseau **Interne**. Trois choix sont possibles correspondant aux trois méthodes de configuration d'un client du Proxy web (partie 8.3) :

- **Détecter automatiquement les paramètres de connexion**
- **Utiliser un script de configuration automatique**
- **Utiliser un serveur Proxy web**

## 7.6 Conclusion

Il est difficile de déterminer quelle configuration est la plus adaptée en ce qui concerne les machines clientes. En effet, ce choix dépend fortement du **type de machines** déployées (Windows, Linux, Mac OS, BSD,...), des **logiciels installés** (notamment des navigateurs), du **niveau de sécurité** nécessaire, de l'**infrastructure** en place (domaine/groupe de travail; DMZ)... Voici un petit tableau récapitulatif des caractéristiques des différents clients :

	<b>Pare-feu</b>	<b>Proxy web</b>	<b>SecureNAT</b>
<b>Authentification des utilisateurs supportée</b>	Oui	Oui si configurée	Non
<b>Système d'exploitation supporté</b>	Windows	Tous	Tous
<b>Protocoles supportés</b>	Tous	HTTP / HTTPS / FTPover HTTP	Tous
<b>Maintenance</b>	contraignante (nécessité de redémarrer le service dans certains cas)	aisée (sauf quand le Proxy est configuré manuellement)	aisée (rien à configurer sauf la passerelle)
<b>Configuration requise sur les clients</b>	installation et configuration d'un logiciel	configuration du navigateur	configuration de la passerelle par défaut

De manière générale, **l'utilisation de clients pare-feu est recommandée**. Sur des configurations exotiques, l'utilisation des clients **SecureNAT** est de mise. Cependant, il peut s'avérer utile du point de vue de la sécurité de configurer les clients SecureNAT en tant que **clients du Proxy web** (pour bénéficier de l'authentification).

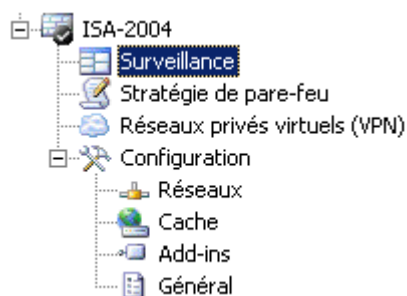
## 8. Surveillance et monitoring d'ISA Server 2004

### 8.1 Introduction

En ce qui concerne les fonctionnalités liées au monitoring, ISA Server 2004 offre peu de nouveautés par rapport à la version 2000 :

- une fenêtre résumant toutes les informations nommée **tableau de bord**
- la possibilité de définir des **vérificateurs de connectivité**
- **l'interface de configuration est bien plus intuitive** que celle de l'utilitaire de gestion ISA 2000
- les **modifications sont toujours appliquées immédiatement**
- par défaut, toutes les données sont stockées dans la base de donnée MSDE plutôt que dans des fichiers.

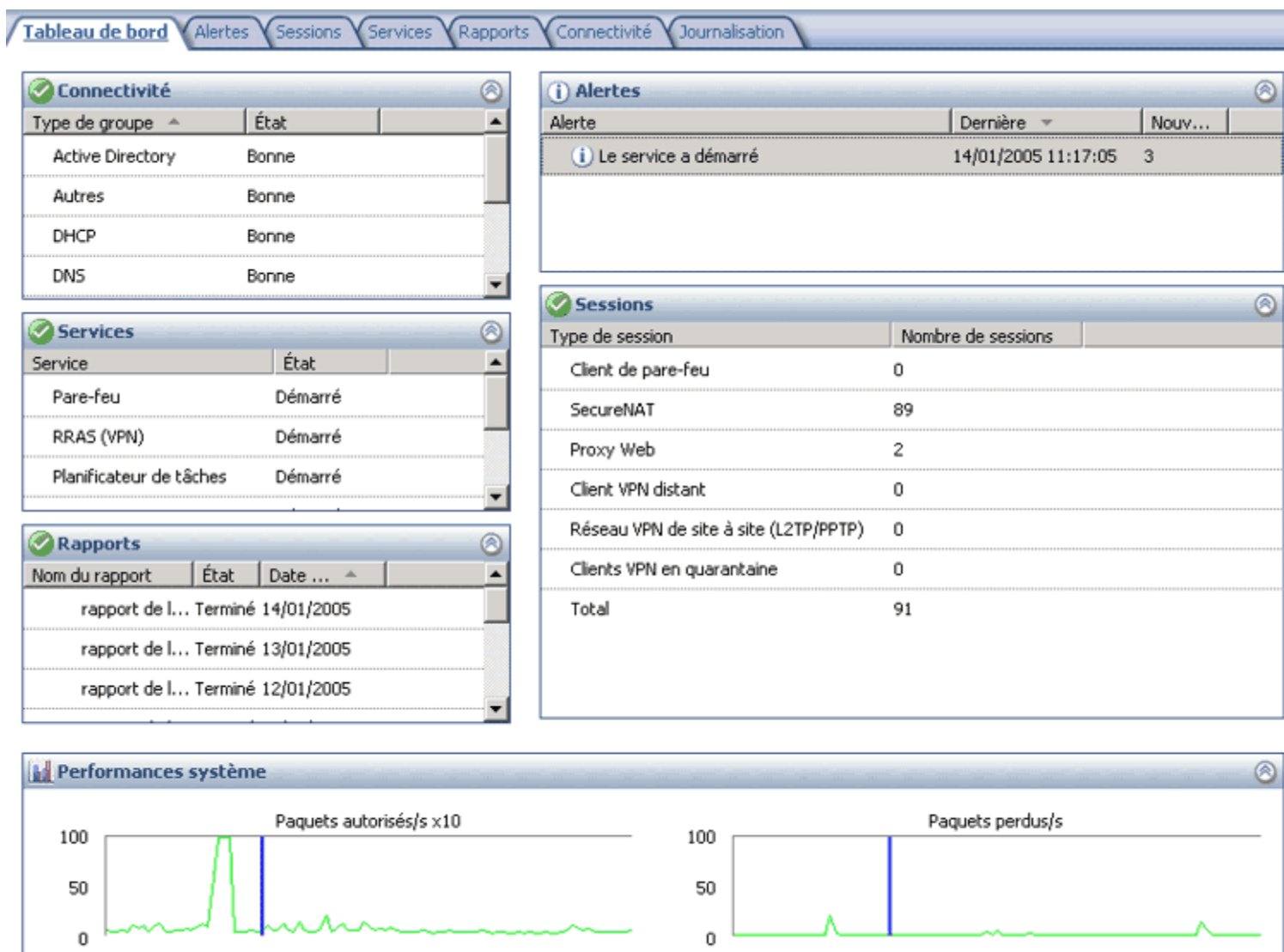
### 8.2 Vue d'ensemble du tableau de bord



Le tableau de bord, accessible à la racine de l'arborescence récapitule les éléments essentiels sur le serveur

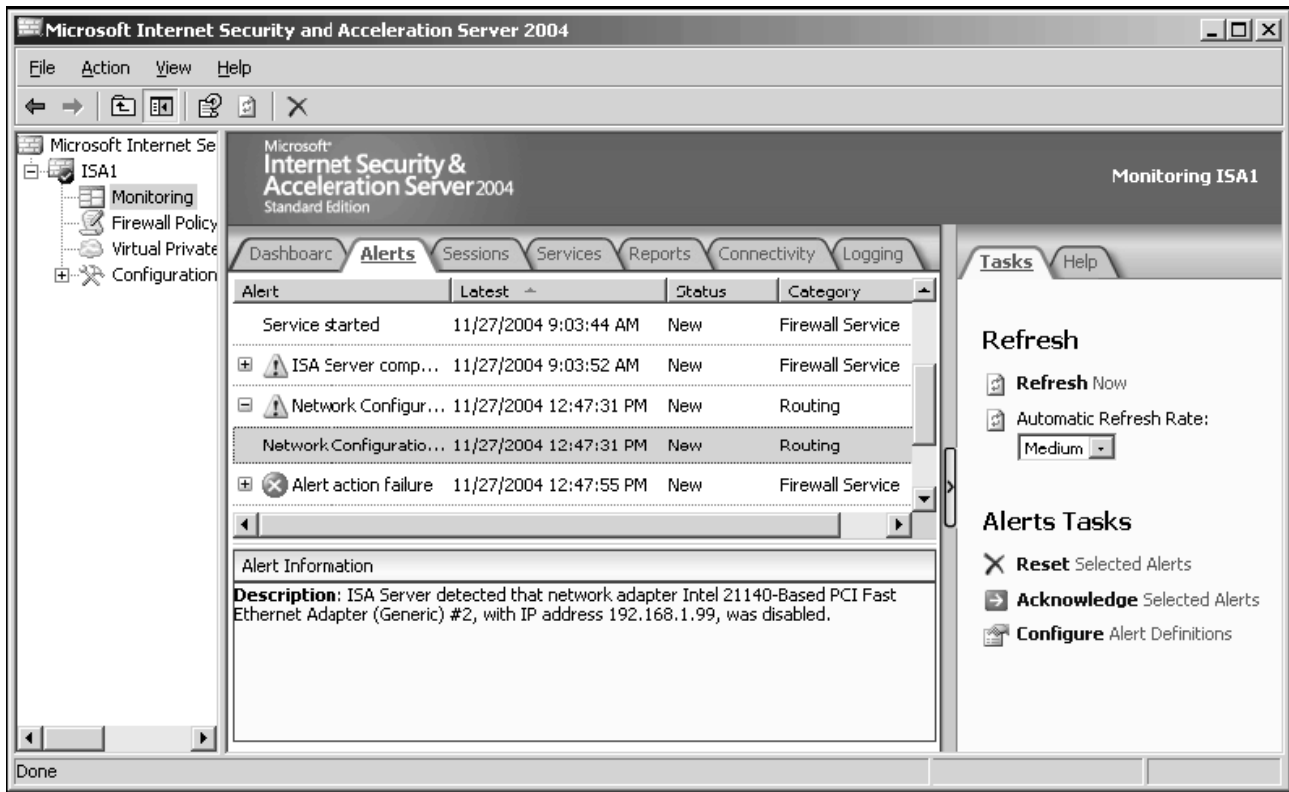
- l'état des **services** et des **vérificateurs de connectivité**
- les derniers **rapports** et **alertes** générés
- les **sessions** actives classées par type
- **l'activité** du serveur

Ce panneau permet de diagnostiquer rapidement un éventuel problème car il se rafraîchit à intervalles réguliers (il est possible de forcer le rafraîchissement).



le tableau de bord d'ISA Server 2004





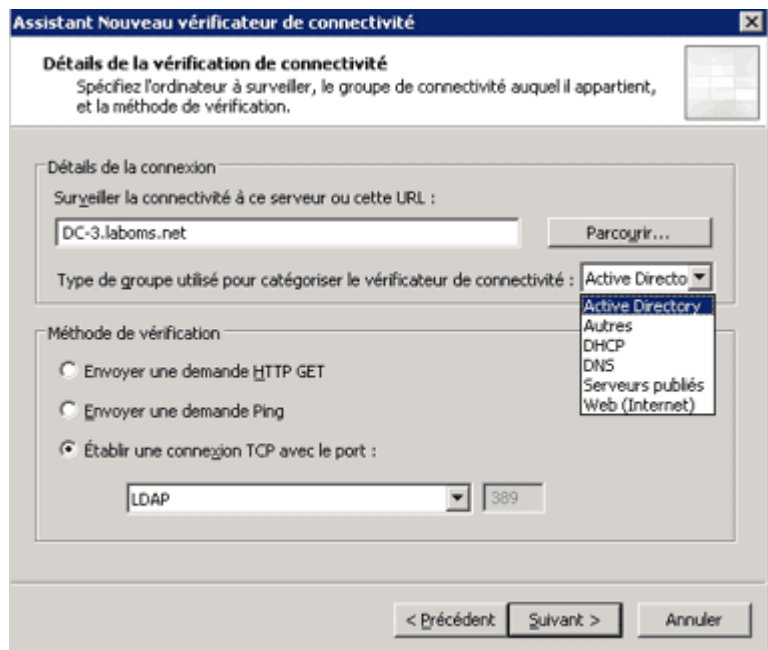
### 8.3 Configuration et utilisation des vérificateurs de connectivité

Les vérificateurs de connectivité permettent de tester l'accessibilité à un serveur ou à une machine donnée. Le test peut prendre plusieurs formes :

- **une requête ICMP** (ping)
- **une requête HTTP**
- une requête sur **un port TCP** choisi par l'administrateur

Certains vérificateurs sont **pré configurés** et accessibles via une liste déroulante :

- **Active Directory** (envoie une requête LDAP au contrôleur de domaine choisi)
- **Autre** (propose une trentaine de port TCP communément utilisés comme FTP, PPTP, POP3, RDP...)
- **DHCP**
- **DNS**
- **Serveurs publiés**
- **Web (Internet)**



## ICMP : Internet Control Message Protocol

Une fois le vérificateur créé, il est possible de **définir un seuil** au-delà duquel l'ordinateur est considéré comme injoignable (dans ce cas, une alerte est générée). La fenêtre connectivité liste les vérificateurs de connectivité et affiche leur état ainsi que diverses autres informations (seuil, type de requête, temps de réponse,...).



Nom du vérificateur ^	Type de groupe	Méthode	Destination	Port	Seuil	Résultat
connexion au contrôleur de domaine	Active Directory	TCP	quigon.matt.lan	389	1000 ms.	<1 ms.
connexion au serveur DHCP	DHCP	Ping	172.16.16.1		1000 ms.	<1 ms.
connexion au serveur DNS primaire	DNS	Ping	212.27.39.2		2000 ms.	Non vérifié (dés)
connexion au site google.fr	Web (Internet)	HTTP	http://www.google.fr		3000 ms.	172 ms.
connexion à la passerelle par défaut	Autres	Ping	81.57.127.254		3000 ms.	32 ms.

## 8.4 Gestion de la journalisation

De la même manière que sous ISA 2000, il est possible de créer automatiquement **des rapports sur l'activité du serveur**. Ils sont générés à partir des informations stockées dans les **fichiers journaux** et permettent notamment de **vérifier les performances de la mise en cache et les accès non souhaités**. Il est très important de **bien choisir les champs qui doivent être sauvegardés** dans les fichiers journaux. En effet par défaut quasiment tous les champs sont sélectionnés, ce qui génère de "gros" fichiers journaux. Voici les fichiers journaux générés par un serveur ISA protégeant un réseau constitué de 35 postes clients sous Windows 2000 professionnel :

Nom ^	Taille	Type	Date de modification	Attributs
ISALOG_20041207_FWS_000.ldf	1 024 Ko	Fichier LDF	08/12/2004 11:09	A
ISALOG_20041207_FWS_000.mdf	670 720 Ko	Fichier MDF	08/12/2004 00:25	A
ISALOG_20041207_WEB_000.ldf	1 024 Ko	Fichier LDF	14/12/2004 07:28	A
ISALOG_20041207_WEB_000.mdf	6 080 Ko	Fichier MDF	14/12/2004 07:28	A
ISALOG_20041208_FWS_000.ldf	1 024 Ko	Fichier LDF	09/12/2004 00:26	A
ISALOG_20041208_FWS_000.mdf	312 768 Ko	Fichier MDF	09/12/2004 00:26	A
ISALOG_20041208_WEB_000.ldf	1 024 Ko	Fichier LDF	09/12/2004 11:36	A
ISALOG_20041208_WEB_000.mdf	3 712 Ko	Fichier MDF	09/12/2004 11:36	A
ISALOG_20041209_FWS_000.ldf	1 024 Ko	Fichier LDF	10/12/2004 13:41	A
ISALOG_20041209_FWS_000.mdf	416 384 Ko	Fichier MDF	10/12/2004 00:24	A

On remarque que l'espace disque utilisé pour stocker les "logs" de trois jours distinct est de 1,4 Go ! Le nombre de champs enregistrés dans la base de données se configure dans l'onglet **Journalisation** de la fenêtre **Surveillance**.

## 8.5 Génération de rapports

Le processus de création de rapport d'ISA Server 2004 est similaire à celui de la version 2000. Il est possible de **générer des rapports mensuels, hebdomadaires, quotidiens** ou bien de les générer manuellement. Lors de la création du rapport un processus nommé **IsaRepGen.exe** parcourt l'intégralité des données de la base et compile les informations pour les rendre exploitables (en créant une page web). Les tâches de rapports ne doivent pas être exécutées au hasard, surtout sur un

serveur en production ! En effet, la création de rapport demande **beaucoup de ressources matérielles** surtout en ce qui concerne le temps processeur, l'utilisation de la mémoire vive et les accès disque. D'où l'intérêt de planifier les tâches de rapport dans une plage horaire où le serveur ISA n'est pas ou peu utilisé (la nuit ou le week-end).

Ci-contre la génération d'un rapport d'activité mensuel sur un serveur ISA gérant 30 machines clientes. **La création a duré environ 2 heures** alors que l'ordinateur utilise un processeur cadencé à 2 GHz, dispose de 512Mo de mémoire vive et utilise un disque dur tournant à 7200 tr/min ! On remarque que le processus accapare : 99% du temps processeur, 230Mo de mémoire vive et 256 Mo de mémoire virtuelle...

Nom de l'image	Nom d'utilisateur	Pr...	Temps ...	Util. mémoire	Taille MV
IsaRepGen.exe	SYSTEM	99	0:33:04	222 736 K	256 560 K
mmc.exe	Administrateur	00	0:00:53	14 012 K	19 520 K
sqlservr.exe	SYSTEM	00	0:02:27	11 788 K	19 504 K
wspssrv.exe	SERVICE RÉSEAU	00	0:01:16	9 804 K	73 300 K
explorer.exe	Administrateur	00	0:09:37	8 036 K	6 000 K
svchost.exe	SYSTEM	00	0:00:08	7 204 K	18 064 K
taskmgr.exe	Administrateur	00	0:00:00	3 508 K	892 K
wmiprvse.exe	SERVICE RÉSEAU	00	0:00:00	2 888 K	2 376 K

Heureusement **ce processus s'exécute en fond de tâche** (et avec une priorité plus faible) ce qui permet au serveur de continuer à répondre aux demandes des clients.

## 8.6 Conclusion

Pour conclure, les capacités de monitoring d'ISA Server 2004 sont identiques à celles de la version 2000 malgré quelques améliorations sensibles en terme d'**ergonomie et de performance** (utilisation de **MSDE** au lieu des fichiers textes pour stocker les données). En revanche il faut se méfier des fonctions de **journalisation** et de **création de rapports** qui demandent :

- **de fortes ressources matérielles**
- **beaucoup d'espace disque**

# 10. Conclusion

En conclusion, ISA Server 2004 s'inscrit dans la lignée de son prédécesseur tout en apportant un grand nombre d'améliorations. On peut citer la nouvelle interface intuitive grâce au système d'onglets et efficace grâce au système d'actualisation (le bouton Appliquer permet de rendre les modifications actives immédiatement ce qui n'était pas le cas sous ISA 2000...). L'intégration totale du serveur VPN dans la console de gestion ISA apporte de nombreux avantages :

- configuration facilitée
- interopérabilité des liaisons sites à sites à l'aide du protocole IPSec tunnel mode
- meilleure sécurité avec le réseau clients VPN en quarantaine

De plus l'assistant modèle réseau ainsi que le nouveau système d'application des règles ont le mérite de clarifier le paramétrage quelque soit le type de règles (d'accès, de chaînage web, de cache,...). Le niveau de sécurité a lui aussi été amélioré de par le système de cryptage entre le nouveau logiciel client pare-feu Microsoft et le serveur ISA, et de par les améliorations effectuées sur les filtres applicatifs et les filtres web. En ce qui concerne le monitoring, la refonte de l'interface et l'ajout des vérificateurs de connectivité et du tableau de bord permettent une meilleure surveillance de l'état et des connexions du serveur.

Quelques remarques assombrissent tout de même ce tableau idyllique :

- la stratégie système s'avère très pratique à l'usage mais reste une faille dans la sécurité du serveur puisqu'elle est activée par défaut
- l'utilisation de MSDE demande plus de ressources matérielles que le système inclus dans ISA 2000
- il n'est pas possible de voir en temps réel toutes les requêtes HTTP/HTTPS/FTP effectuées par les utilisateurs (des systèmes de ce type équipent déjà certains pare-feu matériel, tels ceux de la marque Arkoon, et s'avèrent très pratique à l'usage)
- certaines fonctions avancées pourtant mises en avant par Microsoft déçoivent par leur implémentation difficile. On peut citer le filtre HTTP (aucune méthode, en-tête ou signature HTTP n'est définie par défaut, ce qui oblige l'administrateur à posséder une bonne connaissance du protocole HTTP et à utiliser un analyseur de trames) ou bien encore le système de mise en quarantaine (aucun script n'est fourni par Microsoft et un assistant de configuration aurait été le bienvenue étant donné le nombre d'étapes à réaliser...)