Guide d’installation et de configuration d’Isa Server 2006 :

1 INTRODUCTION : 4

1.1 OBJECTIFS DE CE DOCUMENT : 4
1.2 OU TELECHARGER LA DERNIERE VERSION DE CE DOCUMENT : 4

2 LES NOTIONS INDISPENSABLES POUR DEPLOYER ISA SERVER 2006 : 5

2.1 ADRESSE IP PRIVEE / PUBLIQUE ET LE NAT : 5
2.2 LE ROUTAGE IP : 5
2.3 LES PORTS TCP / UDP ET LES SERVICES RESEAUX ASSOCIES : 5
2.4 LES PARE FEU AVEC ETATS (STATEFULL) ET SANS ETATS (STATELESS) : 5
2.5 COMMENT TESTER ET VALIDER QU'UNE APPLICATION RESEAU EST ACCESSIBLE : 6
2.6 LES PROTOCOLES RESEAUX : 6
2.6.1 Le protocole DNS : 6
2.6.2 Les protocoles web HTTP, FTP : 6
2.6.3 Protocole SMTP 7
2.6.4 Le protocole RDP (Terminal Server mode administration à distance) : 7
2.6.5 Le service d'annuaire Active Directory : 7
2.6.6 Les certificats : 8

3 PRESENTATION D'ISA SERVER 2006 : 9

3.1 PRESENTATION GENERALE : 9
3.2 SCENARIO DE DEPLOIEMENT : 10
3.3 UN PRODUIT EXTENSIBLE : 11
3.4 LE SUCCESSEUR D'ISA SERVER 2006 : 11

4 DEFINIR SON ARCHITECTURE RESEAU CIBLE : 12

4.1 DEFINIR L'ARCHITECTURE CIBLE ISA SERVER 2006 : 12
4.2 ARCHITECTURE DE RESOLUTION DE NOMS DNS : 12
4.3 LE TYPE DE CLIENT ISA SERVER : 12
4.4 QUELQUES SITES WEB SUR ISA SERVER 2006 : 13

5 INSTALLATION D'ISA SERVER 2006 : 14

5.1 INSTALLATION D'ISA SERVER 2006 : 14
5.2 INSTALLER LE SERVICE PACK 1 D'ISA SERVER 2006 : 16
5.3 RENFORCER LA SECURITE D'ISA SERVER 2006 (A FAIRE UNE FOIS TOUTES LES REGLES CONFIGUREES) : 17
5.4 DESACTIVER LE TOE (TCP OFFLOAD ENGINE) 19
5.5 EXECUTER ISA SERVER BEST PRACTICE ANALYSER : 19
5.6 OPTIMISER LES PERFORMANCES D'ISA SERVER 2006 : 20

6 CONFIGURATION DU SERVEUR ISA SERVER 2006 : 21

6.1 CONFIGURATION DES RESEAUX ISA SERVER 2006 : 21
6.1.1 Faire un schéma de son réseau : 21
6.1.2 Les réseaux Isa Server 2006 : 21
6.1.3 Quelques réseaux ISA Server à connaître : 24
6.1.4 Configurer les règles de réseaux : 25
6.2 REGLE D'ACCES OU REGLE DE PUBLICATION : 26
6.3 LES ACCES PAR DEFAUT AU NIVEAU DU SERVEUR ISA SERVER 2006 : 27
6.4 LES STRATEGIES SYSTEMES : 28
6.5 CREATION DE REGLE D'ACCES : 30
6.6 LES REGLES DE PUBLICATION : 32
6.6.1 Création d'une règle de publication de serveur non web : 32
6.6.2 Les règles de publication de serveur web : 34
6.6.3 Configuration des règles de publication web HTTPS et des règles pour publier Outlook Web Access, ActiveSync et Outlook Anywhere : 39

6.7 CONFIGURATION DE LA MISE EN CACHE AVEC ISA SERVER 2006 : 40
6.7.1 Activer le cache sur le serveur Isa Server 2006 : 40
6.7.2 Configurer les règles de cache : 40
6.7.3 Création de tâches de téléchargement de contenu : 41
6.7.4 Gestion du contenu du cache : 41
6.8 CONFIGURATION DE LA DECOUVERTE AUTOMATIQUE : 42
6.9 CONFIGURATION DE LA DETECTION D'INTRUSION : 42
6.10 MISE EN ŒUVRE DU FILTRAGE APPLICATIF AVEC ISA SERVER 2006 : 43
6.10.1 Présentation du filtre applicatif SMTP 44
6.10.2 Présentation du filtre applicatif HTTP : 45

7 LES TACHES D'ADMINISTRATION COURANTE D'ISA SERVER : 46

7.1 SAUVEGARDER SON SERVEUR ISA SERVER : 46
7.2 MISE EN ŒUVRE DE LA DELEGATION D'ADMINISTRATION AVEC ISA SERVER 2006 : 46
7.3 CONFIGURATION DE RAPPORTS AVEC ISA SERVER 2006 : 46
7.4 TROUBLESHOUTING AVEC L'ONGLET SURVEILLANCE\JOURNALISATION : 48

8 MISE EN ŒUVRE DES VPN : 49

8.1.1 Configuration d'Isa Server comme serveur VPN L2TP : 49
8.1.2 Pour créer des connexions VPN site à site : 49

1 Introduction :

1.1 Objectifs de ce document :

Ce document a pour objectif de présenter Isa Server 2006. Il n'est pas exhaustif. Certaines fonctionnalités d'Isa Server comme la configuration d'Isa Server 2006 ne sont pas abordées (peut être dans une prochaine version…).

1.2 Où télécharger la dernière version de ce document :

Ce document peut être téléchargé sur http://msreport.free.fr.

2 Les notions indispensables pour déployer Isa Server 2006 :

2.1 Adresse IP privée / publique et le NAT :

Il existe deux types d'adresses IP :
- Les adresses IP publiques : elles sont routables sur Internet.
- Les adresses IP privées : elles ne sont pas routables sur Internet.

Pour plus d'informations sur les adresses privées / publiques, voir :
- http://www.commentcamarche.net/contents/internet/ip.php3

Un serveur NAT permet à des équipements réseaux avec une adresse IP privée de communiquer avec des équipements réseaux avec une adresse IP publique.
Le NAT permet d'altérer les paquets en remplaçant une adresse IP privée par l'adresse IP publique et inversement.
Attention, certaines protocoles / applications ne supportent pas le NAT comme IPSEC. En effet le NAT modifie le paquet IP alors qu'IPSEC garantit que ce dernier n'a pas été altéré.
Pour plus d'informations sur le NAT, voir :
- http://fr.wikipedia.org/wiki/Network_address_translation
- http://www.commentcamarche.net/contents/internet/nat.php3

Pour utiliser le NAT avec IPSEC, il faut utiliser le protocole NAT-T :
- http://support.microsoft.com/kb/885348/en-us
- http://support.microsoft.com/kb/818043/en-us
- http://www.isaserver.org/tutorials/Allowing-Inbound-L2TPIPSec-NAT-Traversal-Connections-through-Back-Back-ISA-Server-Firewall-DMZPart1.html

2.2 Le routage IP :

Pour plus d'informations sur la notion de routage :
- http://www.frameip.com/routage/

Windows 2003 intègre un service de routage appelé RRAS (Routage et Accès distant). Pour plus d'informations sur le service RRAS, voir http://technet.microsoft.com/fr-fr/library/bb967586.aspx.

2.3 Les ports TCP / UDP et les services réseaux associés :

Chaque application réseau est associée à un ou plusieurs ports TCP / UDP / ICMP.
Un serveur web tourne par exemple sur le port TCP 80. Seule une application peut s'exécuter sur un port TCP / UDP donnée. Dans le cas contraire il y a conflit.
La liste de tous les ports connus est disponible sur un serveur Windows 2003 dans le fichier C:\windows\system32\drivers\etc\services

Pour plus d'informations sur les applications associées à chaque port TCP / UDP :
- http://www.frameip.com/liste-des-ports-tcp-udp/affichage-liste-des-ports-tcp-udp.php?plage=1

2.4 Les pare feu avec états (statefull) et sans états (stateless) :

Il existe deux grandes familles de pare feu :
- Les pare feu sans états : ce type de pare feu nécessite de créer une règle pour le trafic généré par un équipement réseau (requête http par exemple) qui initie la communication et une règle pour l'équipement réseau qui répond.
- Les pare feu avec états : ce type de pare feu nécessite uniquement de créer une règle pour le trafic généré par l'équipement réseau (requête http par exemple) qui initie la communication. La règle correspondant au trafic généré par l'équipement réseau qui répond à la requête est créée dynamiquement par le pare feu avec états.

Isa Server 2006 est un pare feu avec états.
Pour plus d'informations voir http://fr.wikipedia.org/wiki/Pare-feu.

2.5 Comment tester et valider qu'une application réseau est accessible :

Il existe des outils qui permettent de tester les connexions réseaux.

- Telnet (pour les ports TCP uniquement) : exemple : telnet www.google.fr 80)
- ZenMaps (http://nmap.org/zenmap) permet sous Windows de générer des connexions TCP / UDP.

2.6 Les protocoles réseaux :

2.6.1 Le protocole DNS :

Le protocole DNS permet de résoudre des noms complets DNS (FQDN) en adresses IP et inversement. Pour plus d'informations sur le protocole DNS :

- http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=15D276A5-4BF6-4ADD-9F67-56B38CCB576B&displaylang=en

2.6.2 Les protocoles web HTTP, FTP :

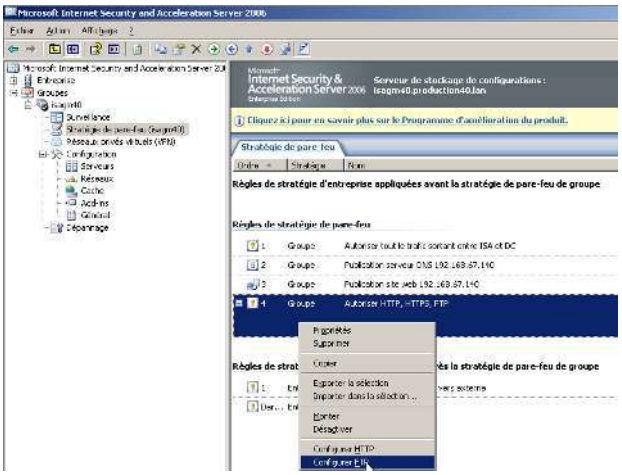
Isa Server 2006 est la solution idéale pour sécuriser les serveurs web IIS 5, 6 et 7 de Microsoft. Il n'est en effet pas prudent de publier directement sur Internet un serveur web IIS (c'est tout aussi vrai pour un serveur web Apache).
Isa Server 2006 permet par exemple de bloquer certaines méthodes HTTP ou de détecter la signature d'un programme pour le bloquer.
Un pré-requis à la mise en œuvre d'Isa Server 2006 est donc de connaître le fonctionnement du protocole HTTP et FTP :

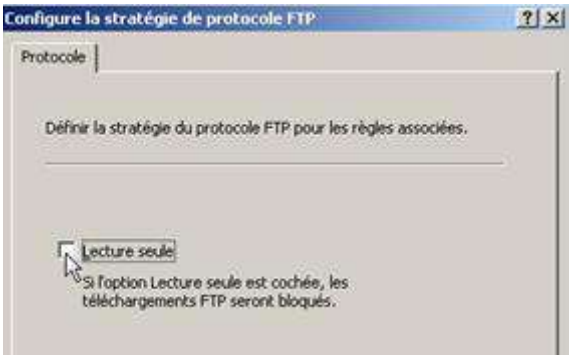
- http://www.commentcamarche.net/contents/internet/http.php3
- http://www.commentcamarche.net/contents/internet/ftp.php3
- http://fr.wikipedia.org/wiki/File_Transfer_Protocol
- http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html
- http://www.webdav.org/specs/rfc2518.html

Pour plus d'informations sur IIS :

- http://www.mmt-fr.org/article283.html
- http://www.lhebergeur.fr/iishelp/iis/htm/core/iiiisin.htm
- http://www.laboratoire-microsoft.org/videos/5359
- http://technet.microsoft.com/fr-fr/library/cc785089(WS.10).aspx

Attention, par défaut Isa Server 2006 bloque l'accès en écriture au site web FTP.
Pour désactiver, cela il faut configurer le filtre applicatif FTP au niveau de la règle d'accès qui autorise le FTP en sortie par exemple.





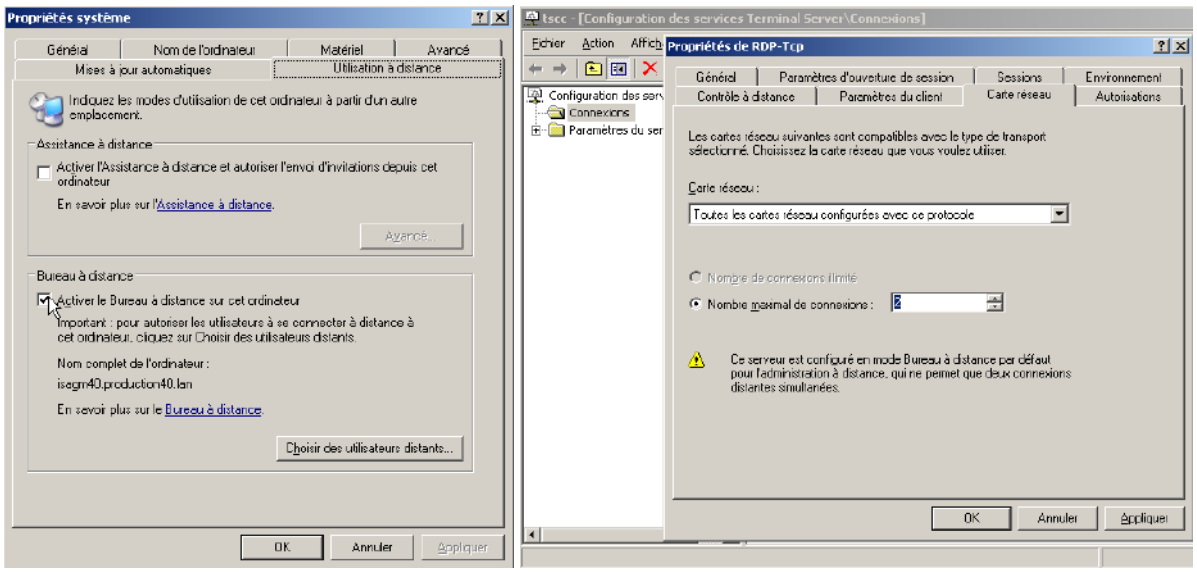
2.6.3 Protocole SMTP

Le protocole SMTP est le protocole standard pour la messagerie.
Isa Server est capable de bloquer certaines méthodes SMTP à l'aide du filtre d'application SMTP intégré nativement dans Isa Server. Pour plus d'informations sur le protocole SMTP :

- http://www.commentcamarche.net/contents/internet/smtp.php3

2.6.4 Le protocole RDP (Terminal Server mode administration à distance) :

Il est utilisé pour permettre la prise en main à distance d'une station de travail (à partir de Windows XP) ou d'un serveur (depuis Windows 2000 Server).
Pour se connecter en bureau à distance, utiliser le client Bureau à distance : MSTSC.EXE.
Pour activer le bureau à distance sur une station de travail ou un serveur, aller dans le panneau de configuration | Système et cliquer sur « *Utilisation à distance* ».
Il peut être intéressant de configurer le protocole RDP pour n'écouter que sur une carte réseau spécifique (sur Windows Server 2000 Server et ultérieur).



Pour plus d'informations :

- http://technet.microsoft.com/en-us/library/cc754746(WS.10).aspx
- http://www.microsoft.com/windowsserver2003/techinfo/overview/quickstart.mspx
- http://support.microsoft.com/kb/324820/en-us

2.6.5 Le service d'annuaire Active Directory :

Isa Server 2006 peut être configuré pour filtrer l'application des règles selon des ensembles d'utilisateurs. Ces derniers peuvent être entre autres des utilisateurs ou des groupes du domaine Active Directory. Pour plus d'informations sur Active Directory :

- http://www.windowsreference.com/dns/step-by-step-guide-for-windows-server-2003-domain-controller-and-dns-server-setup/
- http://msreport.free.fr/?p=85
- http://msreport.free.fr/?p=155

2.6.6 Les certificats :

Pour créer une règle de publication web de type pontage SSL (deux sessions HTTPS), il est nécessaire d'installer un certificat sur le serveur Isa Server 2006.
Isa Server 2006 doit aussi être capable d'établir une connexion HTTPS au serveur web interne sans émettre d'alerte. Pour cela le certificat du serveur web interne doit :

- Ne pas avoir expiré.
- Avoir été généré par une autorité de certification de confiance.
- Contenir le nom avec lequel Isa Server a établi la connexion.

Pour plus d'informations sur les certificats et les autorités de certification :

- http://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman
- http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique
- http://www.laboratoire-microsoft.org/videos/10692/
- http://technet.microsoft.com/fr-fr/library/aa998956(EXCHG.65).aspx

3 Présentation d'Isa Server 2006 :

3.1 Présentation générale :

Isa Server 2006 est :
- Un pare feu qui peut filtrer sur les couches 3, 4 et 7 du modèle OSI.
- Un routeur.
- Un serveur NAT.
- Un serveur VPN.
- Un serveur proxy / reverse proxy.
- Un IDS / IPS (très basique).

Isa Server 2006 existe en deux versions :
- Standard.
- Entreprise.

Le tableau ci-dessous liste les différences entre les deux versions :

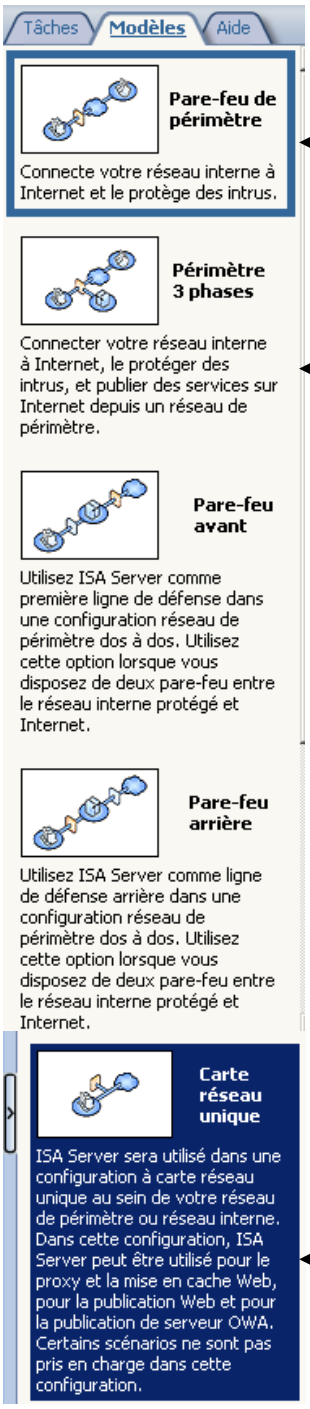
Feature	Standard Edition	Enterprise Edition
Scalability		
Networks	Unlimited	Unlimited Adds enterprise networks
Scale up	Up to 4 CPUs, 2-gigabyte (GB) RAM	Unlimited (per operating system)
Scale out	Single server	Up to 32 nodes through Network Load Balancing
Caching	Single-server store	Unlimited (through Cache Array Routing Protocol [CARP])
Availability		
Windows Network Load Balancing (NLB) Support	Not supported	Yes (integrated)
Manageability		
Policies	Local	Array and enterprise policies use Active Directory Application Mode (ADAM)
Branch office	Through the manual import and export of policy	Enterprise-level and array-level policies
Monitoring/alerting	Single-server monitoring console Microsoft Operations Manager (MOM) Management Pack	Multiserver monitoring console MOM Management Pack
Multiple networks	Templates	Templates

Pour plus d'informations :
- http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/editions.aspx

3.2 Scénario de déploiement :

Isa Server peut être déployé selon plusieurs scénarios :

- Pare feu de périmètre : Dans ce scénario, Isa Server dispose de deux cartes réseaux. Il peut servir pour faire du filtrage (sur les niveaux 3, 4 et 7 de la couche OSI), de serveur proxy (proxy / reverse proxy), d'IDS / IPS et de serveur VPN.
- Pare feu avant / pare feu arrière : ce mode consiste à déployer deux pare feu (de préférence deux modèles différents) entre le réseau interne et le réseau externe. Ce mode de déploiement permet de créer un réseau de périmètre (ou DMZ) entre les deux pare feu. La Best Practice consiste alors à déployer tous les serveurs à publier sur Internet au niveau de la DMZ.
- **Single Network Card : Isa Server dispose alors d'une seule carte réseau. Dans ce mode, Isa Server 2006 fonctionne uniquement comme un serveur proxy et reverse proxy.**



Réseaux standard (2 cartes réseaux)

Permet la création d'une DMZ où l'on héberge les serveurs à publier sur Internet.

Ce n'est plus qu'un proxy et reverse proxy. (Publication et application web).

Pour plus d'informations sur le scénario de déploiement d'Isa Server 2006 avec une seule carte réseau :

- http://technet.microsoft.com/en-us/library/bb794774.aspx
- http://microsoftsolution.blogspot.com/2008/03/configuration-of-isa-server-2006-in.html
- http://www.isaserver.org/tutorials/ISA-Server-2006-Network-Templates.html
- http://technet.microsoft.com/en-us/library/cc302586.aspx

Pour plus d'informations sur les scénarios de déploiement d'Isa Server 2006 :

- http://www.labo-microsoft.com/whitepapers/21518

3.3 Un produit extensible :

Il existe de nombreux plugins qui permettent d'étendre les fonctionnalités d'Isa Server.
Le module additionnel Kaspersky Anti-Virus for Microsoft ISA Server permet par exemple de détecter les virus et les spyware au niveau des flux HTTP et FTP qui transitent à travers Isa Server 2006.
Une liste des modules additionnels pour Isa Server est fournit par le site web http://www.isaserver.org (au niveau de la page d'accueil).

3.4 Le successeur d'Isa Server 2006 :

Le successeur d'Isa Server 2006 s'appelle Forefront Threat Management Gateway (TMG) 2010.
Le programme a été complètement redéveloppé.

Pour plus d'infirmations :

- http://www.microsoft.com/Forefront/edgesecurity/iag/en/us/default.aspx
- http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd
- http://www.mslive.fr/actualites-640-forefront-threat-management-gateway-(tmg)-2010-est-rtm-testez.aspx

4 Définir son architecture réseau cible :

Avant tout déploiement d'Isa Server 2006, il faut définir son architecture cible.

4.1 Définir l'architecture cible Isa Server 2006 :

Avant de se lancer dans l'installation d'Isa Server 2006, il faut déterminer l'architecture réseau cible. Pour cela, il faut répondre aux questions suivantes :

- Quels sont les sous réseaux IP au niveau du réseau local ?
- Quels est le type de relation entre chaque réseau (interne, externe, périmètre) ? Il existe deux types de relation réseau possible, NAT ou ROUTAGE.
- Dois-je créer un réseau de périmètre ?
- Quels sont mes besoins en termes de bande passante ?
- Quel sera le scénario de déploiement d'Isa Server 2006 ?
- Quel est mon budget ?

La majorité des incidents Isa Server sont le fait d'une mauvaise configuration des réseaux Isa Server. Certains clients oublient par exemple de déclarer dans la TAL (dans le réseau Interne d'Isa Server) certains sous réseaux IP du LAN. Isa Server considère alors que ces réseaux sont externes à l'entreprise et refuse alors toutes demandes depuis les machines de ces sous réseaux IP. Ces dernières arrivent en effet via la patte interne de l'ISA alors qu'elles devraient arriver par la patte externe. Pour plus d'informations sur la configuration des réseaux Isa Server 2006, voir :

- http://technet.microsoft.com/fr-fr/library/cc302676(en-us).aspx

4.2 Architecture de résolution de noms DNS :

Un autre point très important concerne la résolution de noms DNS.
Il y a deux grandes écoles :

- Tous les équipements réseaux sur le LAN autres que le serveur ISA ne peuvent pas résoudre les noms DNS externes.
- Les équipements réseaux sur le LAN peuvent résoudre les noms DNS externes. Dans ce cas, il faut créer une règle d'accès qui autorise le protocole DNS (TCP 53 / UDP 53) du réseau interne vers le réseau externe.

Pour plus d'informations :

- http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part1.html
- http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part2.html
- http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part3.html
- http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part4.html

4.3 Le type de client Isa Server :

Isa Server 2006 dispose de trois types de client :

- Le client proxy web : il permet d'utiliser le moteur proxy d'Isa Server. Ce client permet de filtrer uniquement l'accès aux sites web HTTP, HTTPS et FTP. Le client proxy web permet de filtrer sur des ensembles d'utilisateurs.
- Le client Secure NAT : il permet d'utiliser le moteur de routage / NAT d'Isa Server 2006 et donc de filtrer les accès à tous les protocoles. Il ne permet pas de filtrer sur des ensembles d'utilisateurs. Pour être client Secure NAT, le flux réseau doit transiter par le serveur Isa Server. Le cas le plus simple est celui d'une station de travail qui a Isa Server comme passerelle par défaut.
- Le client pare feu : il s'agit d'un logiciel à déployer sur toutes les stations de travail Windows. Ce dernier est disponible sur le CD d'installation dans le dossier client ou sur Internet. http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=05C2C932-B15A-4990-B525-66380743DA89

Ce type de client permet de filtrer les accès à tous les protocoles et d'utiliser le filtrage sur les ensembles d'utilisateurs.

4.4 Quelques sites web sur Isa Server 2006 :

Site web français :

- http://technet.microsoft.com/fr-fr/forefront/edgesecurity/bb758895.aspx
- http://www.microsoft.com/france/Vision/Recherche.aspx?Qry=&S=x&Did=&Pid=611c646f-3a25-4594-8c6a-6daff00e1a0b&Nid=&Cid=&Tid=&x=52&y=6
- http://technet.microsoft.com/fr-fr/forefront/edgesecurity/bb758895.aspx
- http://www.labo-microsoft.com/articles/server/ISA2004/
- http://www.labo-microsoft.com/whitepapers/isa_server_2000_et_2004

Site web Technet anglais :

- http://technet.microsoft.com/en-us/library/bb898433.aspx
- http://www.isaserver.org/
- http://technet.microsoft.com/fr-fr/forefront/edgesecurity/bb734830.aspx

5 Installation d'Isa Server 2006 :

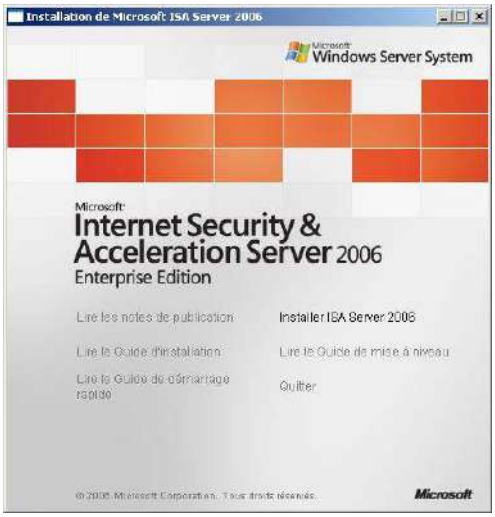
Les étapes suivantes doivent être effectuées lors d'une installation d'Isa Server 2006 :
- Installer Windows 2003 SP2 + derniers correctifs.
- Installer Isa Server 2006.
- Installer le service pack 1 d'Isa Server 2006.
- Sécuriser le serveur Isa Server 2006 (documenter et former l'équipe d'administration du client). A faire après avoir configurer toutes les règles de filtrage et activer toutes les fonctionnalités (VPN…).
- Désactiver le TOE.
- Exécuter *Isa Server Best Practice Analyser*.
- Optimiser les performances d'Isa Server 2006.

Remarque :
- Ne pas définir de passerelle par défaut sur la carte réseau interne d'Isa Server 2006.

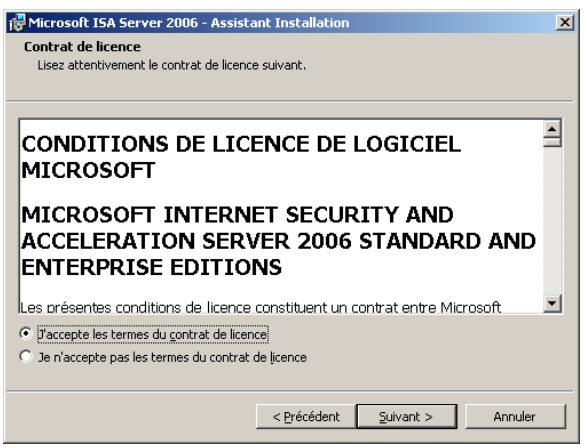
5.1 Installation d'Isa Server 2006 :

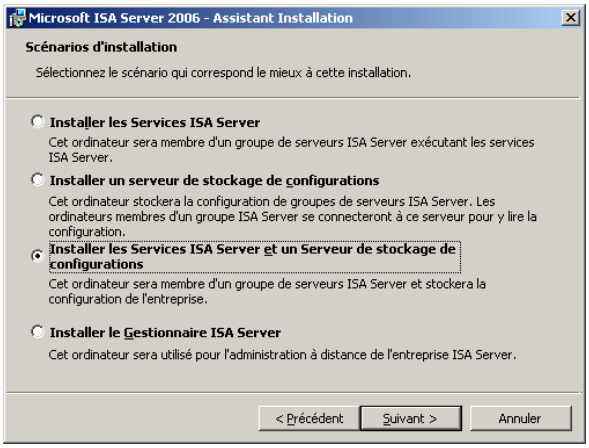
Les sources d'installation d'Isa Server 2006 peuvent être téléchargées à l'adresse suivante :
- http://www.microsoft.com/downloads/details.aspx?familyid=6331154B-A923-45DD-8520-48B63B6BE97B&displaylang=fr

Avant de lancer l'installation d'Isa Server 2006, vérifier que votre serveur respecte les pré-requis pour l'installation d'Isa Server 2006.
- http://technet.microsoft.com/en-us/library/cc304520.aspx

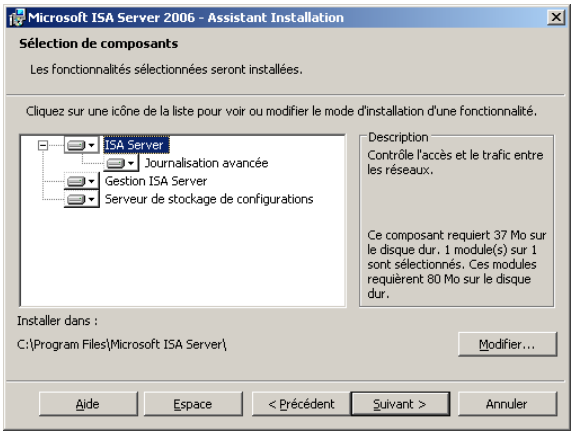


Dans notre cas, nous allons installé le premier serveur Isa Server 2006 Entreprise Edition.
Il nous faut donc installer un serveur de stockage de configuration et les services Isa Server 2006.

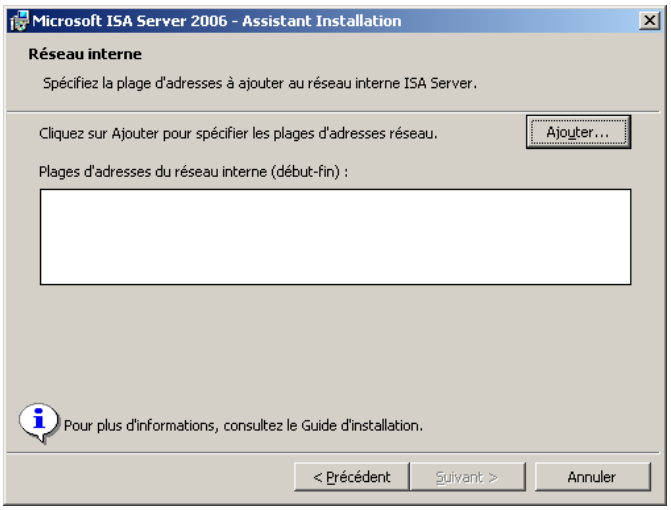


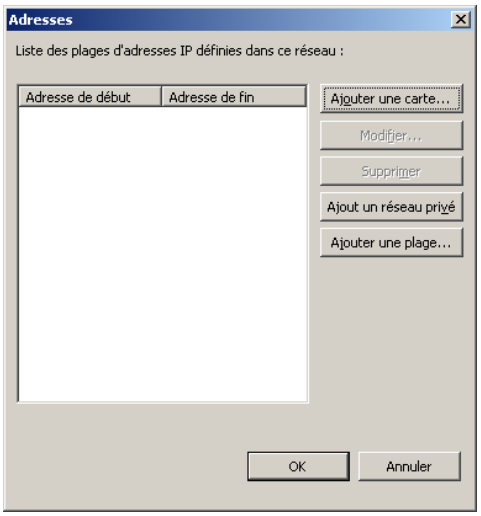


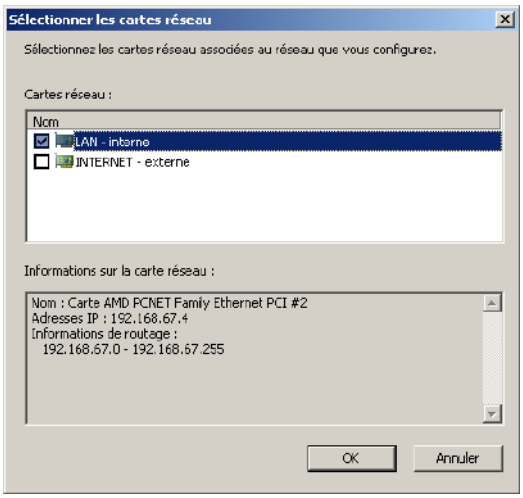
Nous allons créer un nouveau Isa Server 2006 Entreprise.
Nous verrons par la suite que nous pourrons créer des règles d'entreprise et des règles pour des groupes Isa Server.

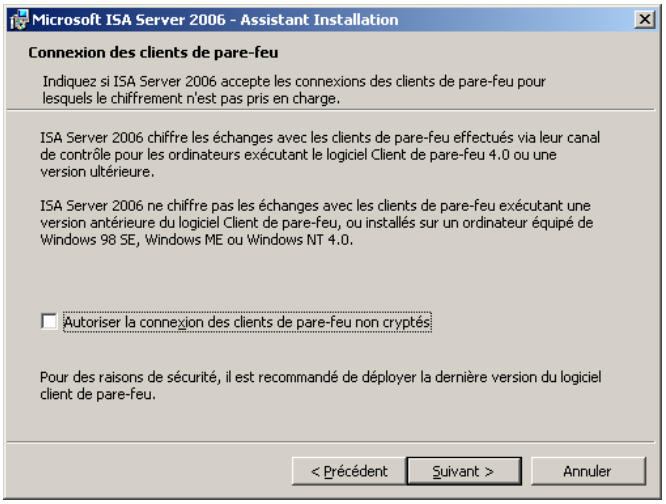


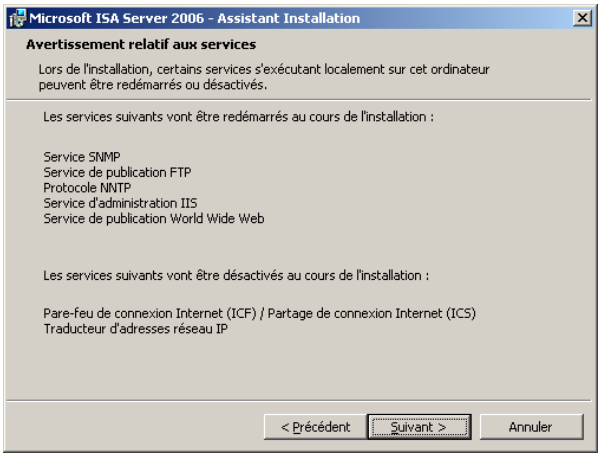
L'étape ci-dessous permet de configurer le réseau interne de l'Isa Server 2006.
La TAL (Table d'adresses locales) correspond en fait aux plages d'adresses IP du réseau interne.
Attention, vous devez ajouter tous les sous réseaux IP de votre LAN et pas seulement le sous réseau IP correspondant à la patte interne de votre Isa Server 2006.

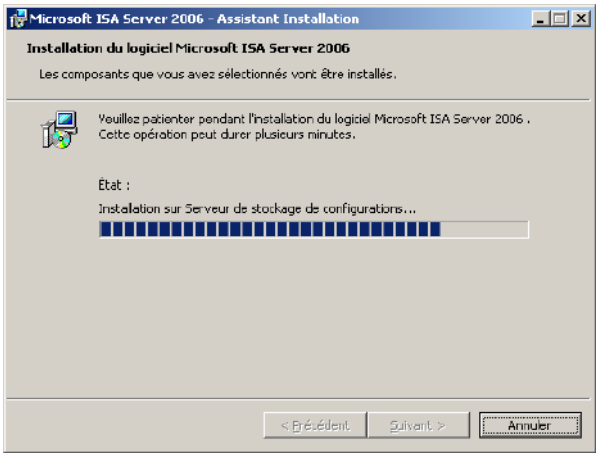












Pour plus d'informations :

- http://technet.microsoft.com/en-us/library/bb794846.aspx
- http://technet.microsoft.com/en-us/library/bb794856.aspx

5.2 Installer le service pack 1 d'Isa Server 2006 :

Installer le service pack 1 est très fortement recommandé. Il apporte de nombreuses fonctionnalités et corrections de bugs dont :

- Le suivi des modifications de la configuration : cela permet d'enregistrer toutes les modifications de configuration appliquées à ISA Server. **Penser à créer des comptes d'administration Isa Server nominatif pour bénéficier pleinement de cette fonctionnalité.**
- Le bouton *Tester* : teste la cohérence d'une règle de publication Web entre le serveur publié et ISA Server.
- Le simulateur de trafic : simule le trafic réseau conformément à des paramètres de demande spécifiques, tels qu'un utilisateur interne et le serveur Web, et fournit des informations sur les règles de stratégie du pare-feu évaluées pour la demande.
- La visionneuse Journalisation des diagnostics : désormais intégrée comme onglet dans la Console d'administration d'ISA Server, cette fonction affiche des événements détaillés sur l'évolution d'un paquet et fournit des informations sur le traitement et la mise en correspondance d'une règle.
- La prise en charge du mode d'équilibrage de charge réseau intégré en trois modes, dont monodiffusion, multidiffusion et multidiffusion avec protocole IGMP (Internet Group Management Protocol). Auparavant, ISA Server n'intégrait que le mode monodiffusion pris en charge par l'équilibrage de charge réseau.
- La prise en charge de l'utilisation de certificats de serveur contenant plusieurs entrées SAN (Subject Alternative Name). Auparavant, ISA Server était en mesure d'utiliser soit uniquement le nom de l'objet (nom commun) d'un certificat de serveur, ou la première entrée de la liste SAN

(Subject Alternative Name). **Cette fonction est très importante surtout si vous souhaitez publier Outlook Anywhere (Exchange 2007).**
- La prise en charge de l'authentification entre les domaines à l'aide de la délégation Kerberos contrainte (KCD). Les informations d'identification des utilisateurs situés dans un autre domaine qu'ISA Server mais dans la même forêt peuvent désormais être déléguées à un site Web publié interne à l'aide de la délégation Kerberos contrainte.

Le service pack 1 d'Isa Server 2006 peut être téléchargé à cette adresse :
- http://www.microsoft.com/downloads/details.aspx?FamilyID=d2feca6d-81d7-430a-9b2d-b070a5f6ae50&displaylang=fr

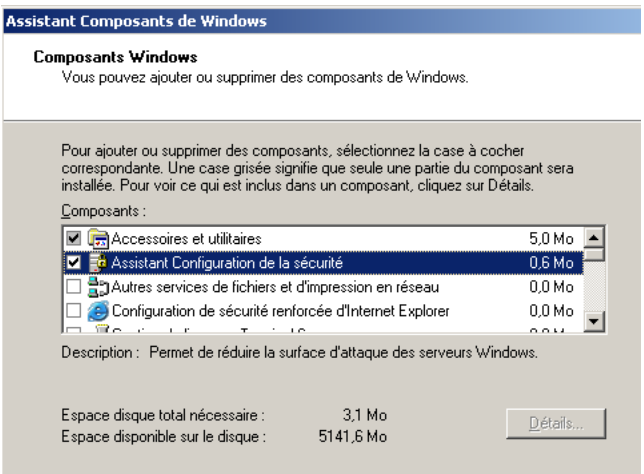
Pour plus d'informations sur les nouveautés du service pack 1 :
- http://www.isaserver.org/tutorials/New-ISA-Firewall-2006-Service-Pack1-Part1.html
- http://www.isaserver.org/tutorials/New-ISA-Firewall-2006-Service-Pack1-Part2.html
- http://technet.microsoft.com/en-us/library/cc707227.aspx

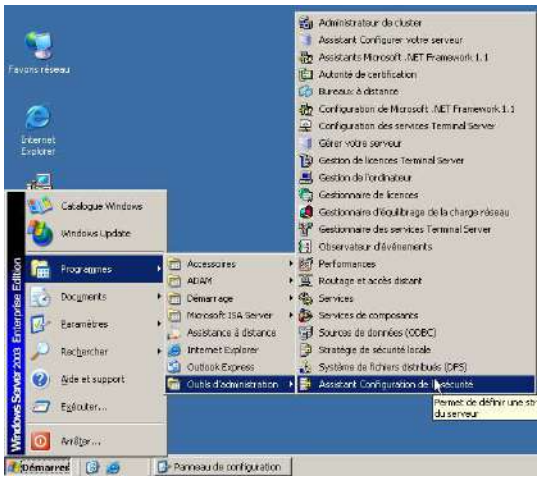
Pour déterminer le niveau de service pack de chaque composant d'Isa Server 2006 :
- http://www.isaserver.org/tutorials/Determine-Correct-ISA-Server-Version-Service-Pack-Information.html

5.3 Renforcer la sécurité d'Isa Server 2006 (à faire une fois toutes les règles configurées) :

Microsoft préconise de dédier un serveur à Isa Server 2006. Les services Windows non nécessaires au fonctionnement d'Isa Server peuvent donc être désactivés afin de réduire la surface d'attaque. Attention ce type de paramétrage étant très complexe, il est préconisé :
- De valider sur maquette le bon fonctionnement d'Isa Server avec ce paramétrage.
- De documenter ce paramétrage.
- De former les équipes d'administration du client.
- En cas d'ouverture d'incident au support Microsoft, pensez toujours à signaler que l'assistant de configuration renforcé de la sécurité à été exécutée sur le serveur Isa Server 2006.

L'article suivant explique comment renforcer la sécurité du serveur Isa Server 2006 :
- http://technet.microsoft.com/fr-fr/magazine/2008.09.isahardening.aspx



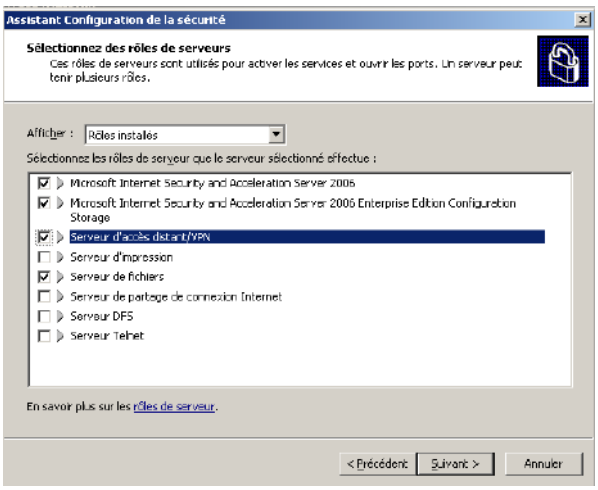


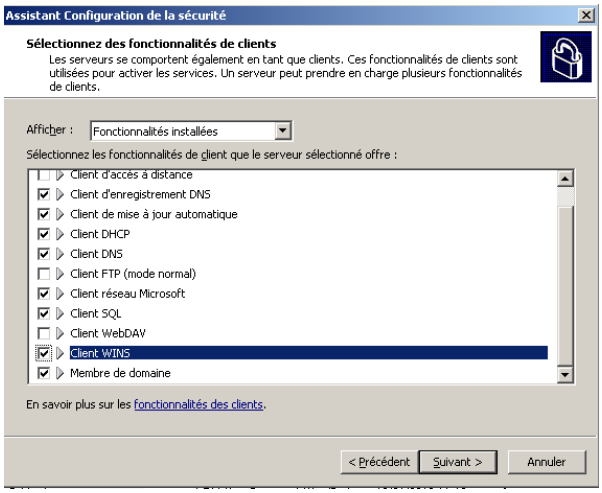
Penser à télécharger la mise à jour de l'assistant de configuration de la sécurité pour Isa Server 2006.
- http://www.microsoft.com/downloads/details.aspx?familyid=2748a927-bd3c-4d87-80fa-8687d5e2ab35&displaylang=en

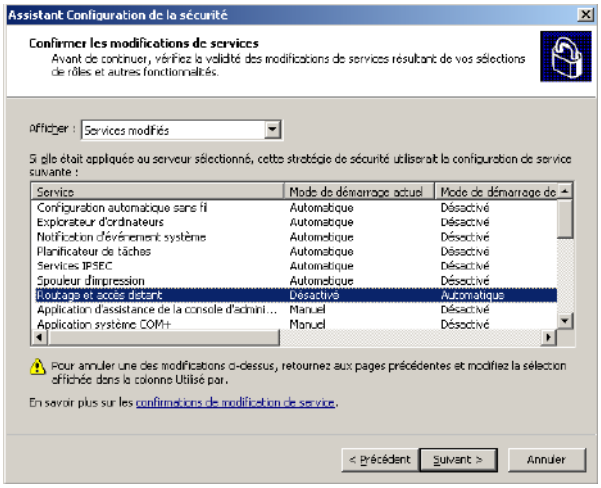
Ouvrir ensuite le document IsaScwHlp.doc et appliquer la procédure indiquée.

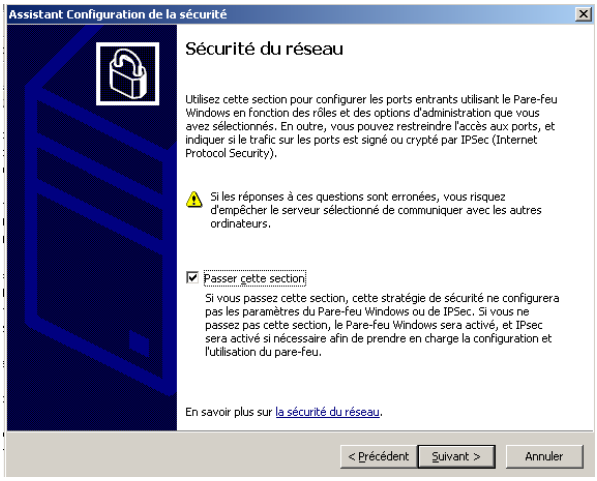
Attention, si le serveur Isa Server 2006 est membre du domaine, penser à autoriser les services nécessaires au bon fonctionnement du domaine !
Si le serveur Isa est serveur VPN aussi, pensez à autoriser le service VPN. Le VPN d'Isa Server 2006 s'appuie en effet sur le service RRAS de Windows 2003 Server.

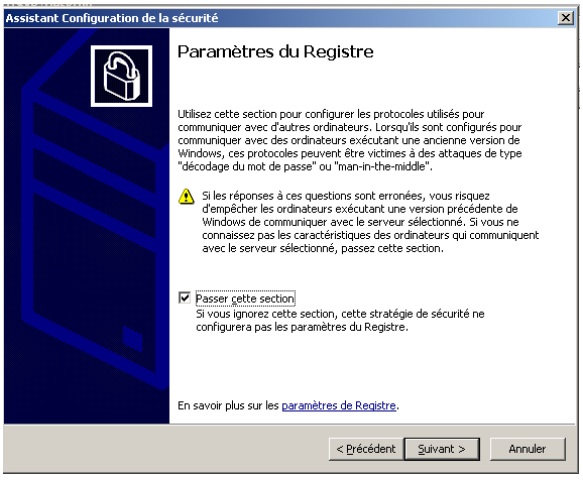
Penser à sélectionner le service client DHCP. C'est lui qui gère la mise à jour dynamique DNS. Ce service doit être démarré !

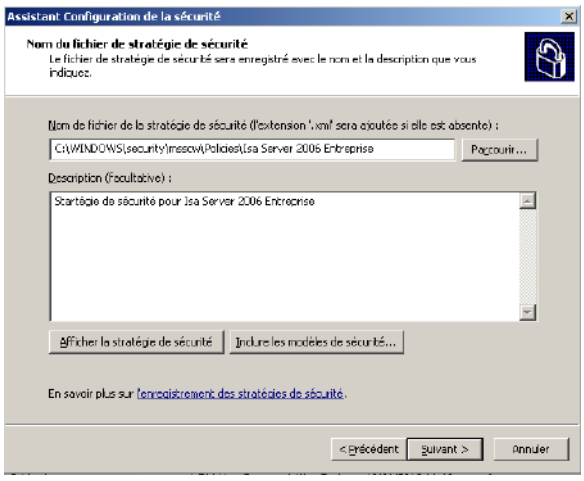


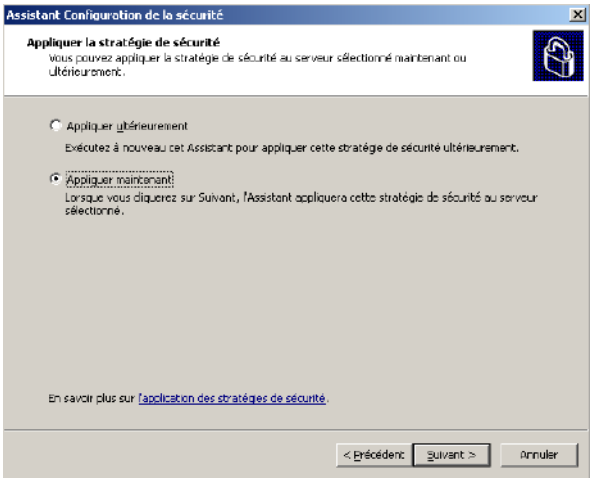












5.4 Désactiver le TOE (TCP Offload Engine)

Le service pack 2 de Windows 2003 Server active par défauts les nouvelles fonctionnalités de TOE (TCP Offload Engine). Hors ces fonctionnalités sont incompatibles avec Isa Server 2006.

Type de l'événement : Avertissement
Source de l'événement : Microsoft ISA Server Control
Catégorie de l'événement : Aucun
ID de l'événement : 30520
Date : 07/02/2010
Heure : 12:11:47
Utilisateur : N/A
Ordinateur : ISAGM40
Description :
Windows Server 2003 Scalable Network Pack, qui est inclus dans Windows Server 2003 Service Pack 2, est activé. Certaines fonctionnalités d'ISA Server ne fonctionnent pas correctement si une carte réseau installée sur un ordinateur ISA Server prend en charge et utilise les fonctionnalités du Scalable Network Pack. Pour plus d'informations, voir l'article 948496 de la Base de connaissances Microsoft. Si vous ne possédez pas de carte réseau prenant en charge les fonctionnalités du Scalable Network Pack, vous pouvez désactiver l'alerte active Windows Server 2003 Scalable Network Pack.

Une Best Practice est donc de désactiver ces fonctionnalités. Pour plus d'informations, voir :
- http://isafirewalls.org/blogs/isa/archive/2007/03/29/attention-il-y-a-qque-soucis-isa-server-avec-le-sp2-de-windows-2003.aspx
- http://msreport.free.fr/?p=163

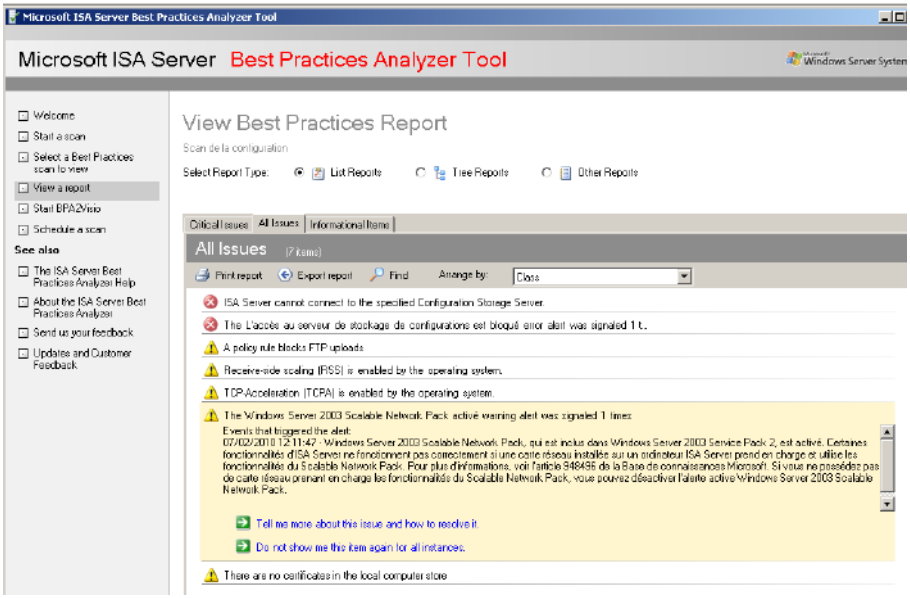
Pour plus d'informations sur le TOE, voir :
- http://en.wikipedia.org/wiki/TCP_Offload_Engine

5.5 Exécuter Isa Server Best Practice Analyser :

Le Best Practice Analyser peut être téléchargé à l'adresse suivante :
- http://www.microsoft.com/downloads/details.aspx?FamilyId=D22EC2B9-4CD3-4BB6-91EC-0829E5F84063&displaylang=en

Lancer un scan et afficher le rapport ensuite.

Dans l'exemple ci-dessous, le Best Practice Analyser remonte entre le fait que l'on n'a pas désactivé le pack SNP de Windows 2003 SP2.



Attention dans certains cas, Isa Server peut remonter des faux positifs ou encore remonter un problème qui a été corrigé.
Purger le contenu du journal application (où est référencée l'erreur) permet de faire disparaître certaines entrées du Best Practice Analyser.

Pour plus d'informations sur le Best Practice Analyser Tool :

- http://www.isaserver.org/tutorials/ISA-Best-Practices-Analyzer-Visio.html

5.6 Optimiser les performances d'Isa Server 2006 :

Appliquer les préconisations de l'article Microsoft suivant :

- http://www.isaserver.org/tutorials/Optimizing-ISA-performance-Part2.html

6 Configuration du serveur Isa Server 2006 :

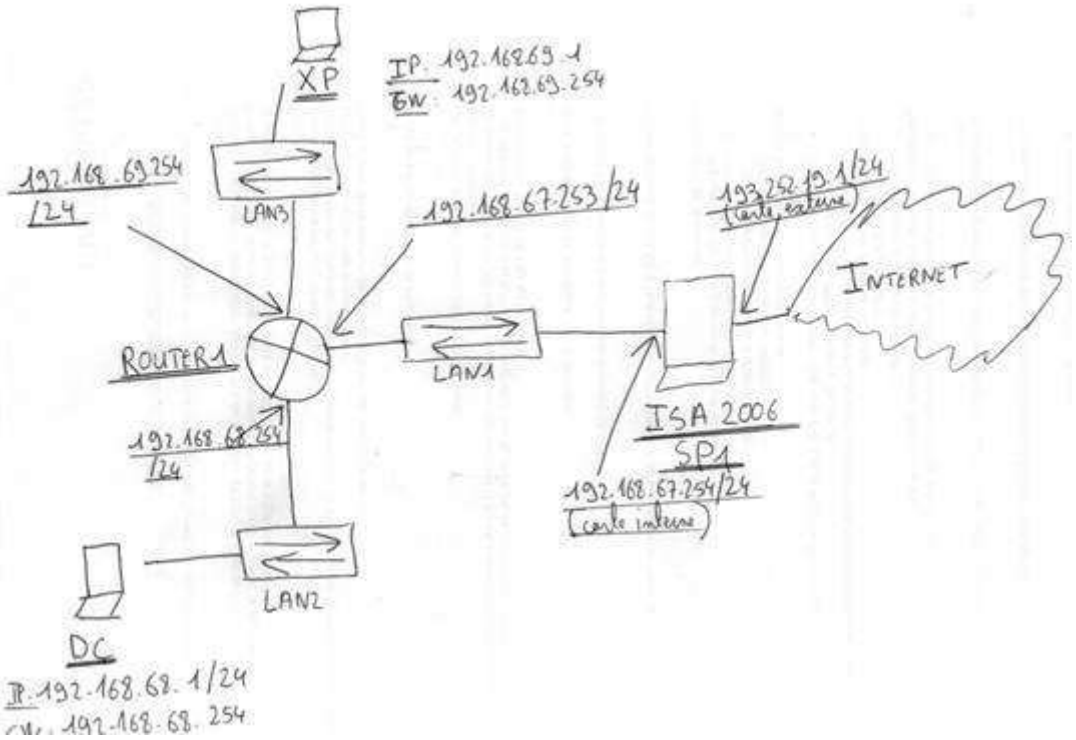
Pour découvrir Isa Server, je vous préconise la lecture des articles SUPINFO suivants :
- http://www.labo-microsoft.com/articles/server/ISA2004/
- http://www.labo-microsoft.com/whitepapers/isa_server_2000_et_2004

6.1 Configuration des réseaux Isa Server 2006 :

Dans cette partie nous allons voir comment :
- Lister les principaux réseaux Isa Server 2006.
- Créer et configurer les réseaux Isa Server 2006.
- Comment configurer les règles de réseau Isa Server 2006 (NAT ou routage).

6.1.1 Faire un schéma de son réseau :

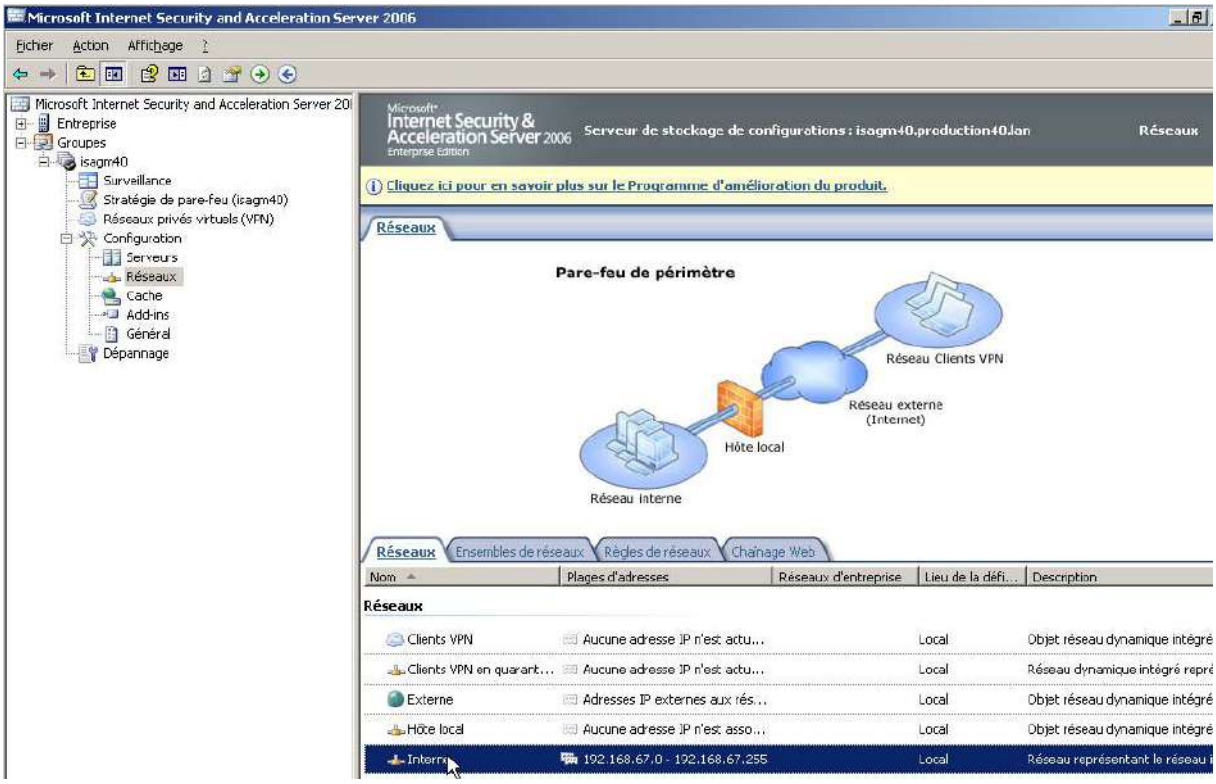
Tout d'abord, il nous faut un schéma de notre réseau.



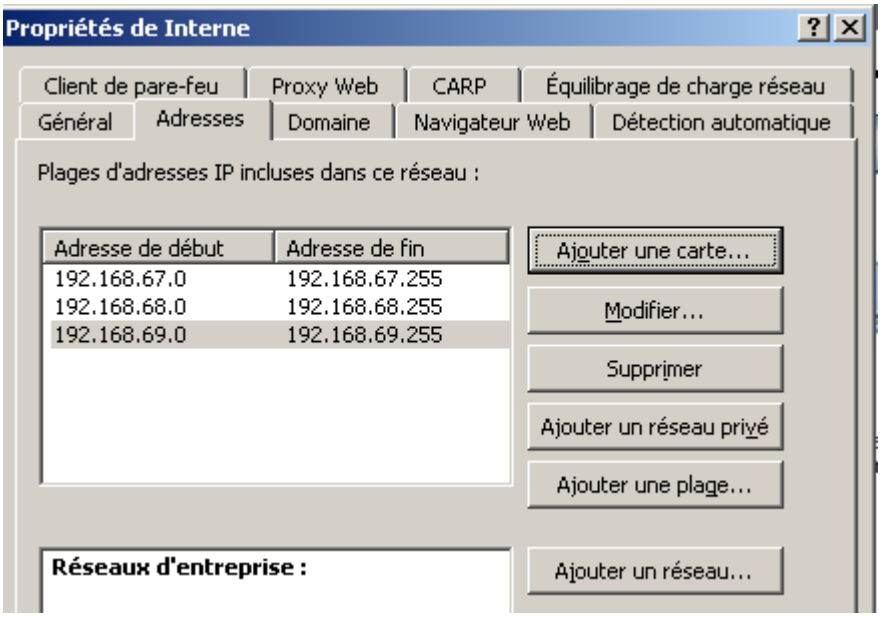
Dans notre cas, le réseau local est divisé en trois sous réseaux IP :
- 192.168.67.0 /24
- 192.168.68.0 / 24
- 192.168.69.0 / 24

6.1.2 Les réseaux Isa Server 2006 :

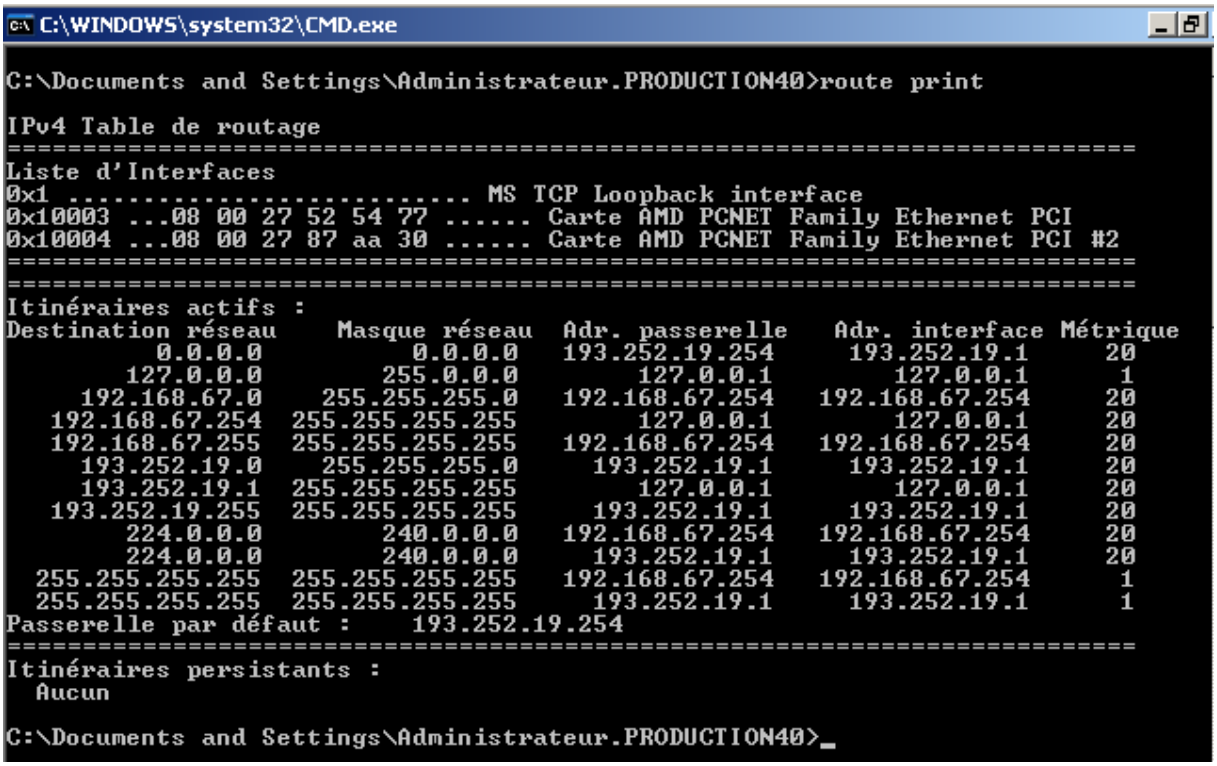
Attention, Isa Server 2006 ne peut filtrer le trafic qu'entre deux réseaux Isa Server 2006.
Il est donc important de bien définir les réseaux Isa Server (toute la complexité d'Isa Server 2006 est là). A l'installation, on doit saisir la TAL (Table d'adresses locales). Cette TAL correspond en fait au réseau INTERNE d'Isa Server.



Dans notre cas, le réseau interne doit donc être configuré de la manière suivante :



Attention, il faut que la configuration des réseaux Isa Server (dont le réseau INTERNE) soit cohérente avec la table de routage du serveur ISA SERVER 2006.
Pour cela, aller dans l'invite de commande Windows et taper la commande *ROUTE PRINT*.



Dans notre cas Isa Server 2006 dispose de deux cartes réseau :

- La carte réseau interne est en 192.168.67.254/24 (adresse IP privée).
- La carte réseau externe est en 193.252.19.1/24 (adresse IP publique)
- La passerelle par défaut sur la carte externe est 193.252.19.254 (adresse IP publique).
- Il n'y a pas de route statique.

Dans notre cas le serveur ISA a donc une carte réseau sur Internet (adresse IP publique).
La relation réseau entre le réseau interne et externe doit donc être NAT car le sous réseau IP interne est en adressage IP privé.

Il y a cependant une erreur de configuration dans la table de routage.
Les réseaux 192.168.68.0/24 et 192.168.69.0/24 ne sont pas déclarées et sont donc considérées comme des sous réseaux externes.

D'après le schéma, ces réseaux sont accessibles depuis Isa Server **via le routeur en 192.168.67.253.** Pour rappel, il est interdit de définir une passerelle par défaut au niveau de la carte réseau interne d'Isa Server 2006. Nous allons donc ajouter des routes statiques vers les réseaux 192.168.68.0 et 192.168.69.0.
Pour cela, il faut taper les commandes suivantes :

- Route add 192.168.68.0 mask 255.255.255.0 192.168.67.253 -p
- Route add 192.168.69.0 mask 255.255.255.0 192.168.67.253 -p

On affiche ensuite la table de routage avec la commande *route print*.

```
C:\Documents and Settings\Administrateur.PRODUCTION40>Route add 192.168.68.0 mas
k 255.255.255.0 192.168.67.253 -p

C:\Documents and Settings\Administrateur.PRODUCTION40>Route add 192.168.69.0 mas
k 255.255.255.0 192.168.67.253 -p

C:\Documents and Settings\Administrateur.PRODUCTION40>route print

IPv4 Table de routage
===========================================================================
Liste d'Interfaces
0x1 ........................... MS TCP Loopback interface
0x10003 ...08 00 27 52 54 77 ...... Carte AMD PCNET Family Ethernet PCI
0x10004 ...08 00 27 87 aa 30 ...... Carte AMD PCNET Family Ethernet PCI #2
===========================================================================
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0   193.252.19.254     193.252.19.1     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
    192.168.67.0    255.255.255.0   192.168.67.254   192.168.67.254     20
   192.168.67.254  255.255.255.255        127.0.0.1        127.0.0.1     20
   192.168.67.255  255.255.255.255   192.168.67.254   192.168.67.254     20
    192.168.68.0    255.255.255.0   192.168.67.253   192.168.67.254      1
    192.168.69.0    255.255.255.0   192.168.67.253   192.168.67.254      1
    193.252.19.0    255.255.255.0     193.252.19.1     193.252.19.1     20
    193.252.19.1  255.255.255.255        127.0.0.1        127.0.0.1     20
  193.252.19.255  255.255.255.255     193.252.19.1     193.252.19.1     20
        224.0.0.0        240.0.0.0   192.168.67.254   192.168.67.254     20
        224.0.0.0        240.0.0.0     193.252.19.1     193.252.19.1     20
  255.255.255.255  255.255.255.255   192.168.67.254   192.168.67.254      1
  255.255.255.255  255.255.255.255     193.252.19.1     193.252.19.1      1
Passerelle par défaut :    193.252.19.254
===========================================================================
Itinéraires persistants :
  Adresse réseau    Masque réseau  Adresse passerelle Métrique
    192.168.68.0    255.255.255.0   192.168.67.253       1
    192.168.69.0    255.255.255.0   192.168.67.253       1

C:\Documents and Settings\Administrateur.PRODUCTION40>_
```

Pour plus d'informations sur la configuration des réseaux Isa Server 2006, voir :

- http://technet.microsoft.com/fr-fr/library/cc302676(en-us).aspx
- http://technet.microsoft.com/en-us/library/bb794774.aspx
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part1.html
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part2.html
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part3.html

6.1.3 Quelques réseaux ISA Server à connaître :

- Hôte local : c'est le serveur ISA Server
- Client VPN : ce sont tous les clients externes qui ont établis une connexion en VPN sur le serveur Isa Server 2006.
- Client VPN en quarantaine : ce sont tous les clients externes qui ont établis une connexion en VPN sur le serveur Isa Server 2006 et qui sont en quarantaine (la fonction de quarantaine VPN est désactivée par défaut dans Isa Server 2006).

Cela veut donc dire qu'il est possible de filtrer le trafic par exemple entre autres entre :

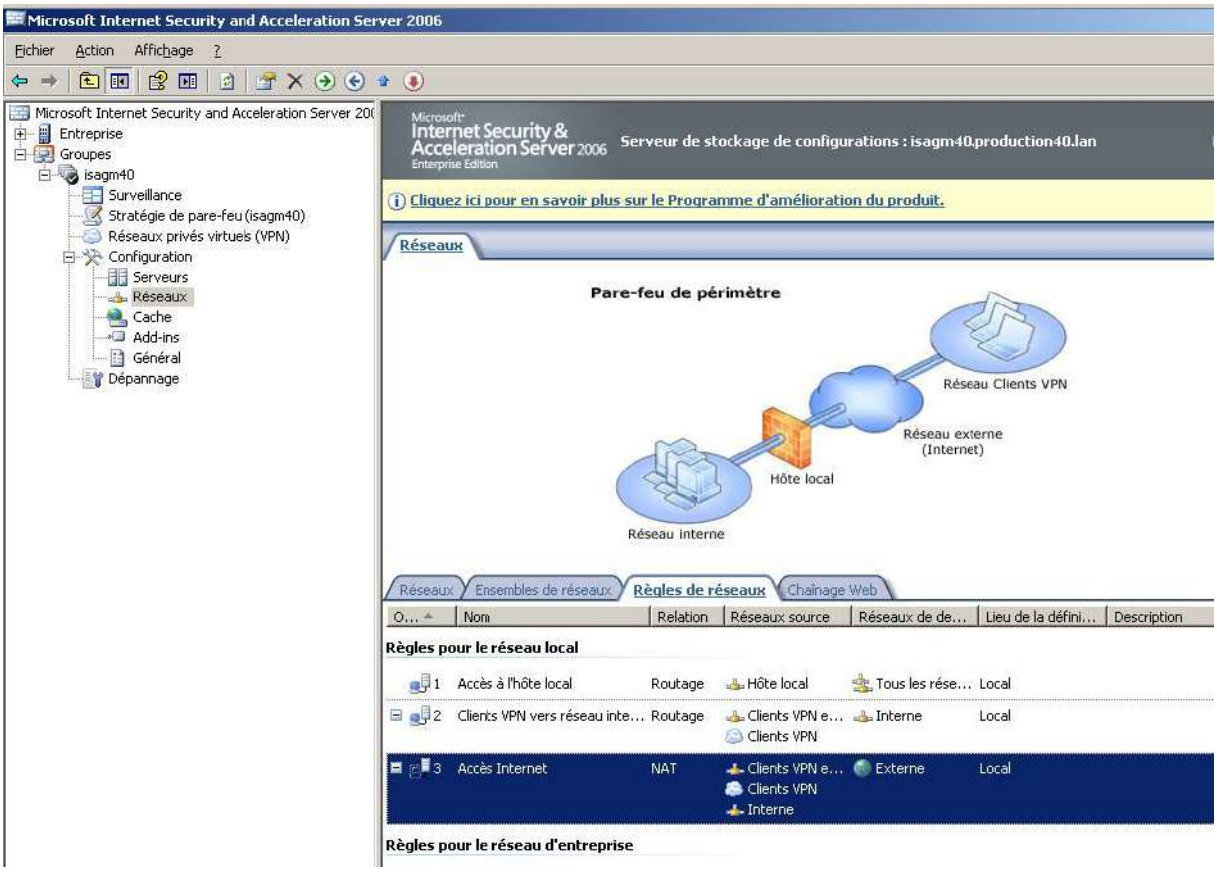
- Le réseau interne et le serveur Isa Server 2006 (réseau hôte local).
- Le réseau VPN et le réseau interne. Il sera donc nécessaire de créer des règles d'accès pour permettre au client VPN d'accéder aux applications / serveurs sur le réseau interne ou d'accéder à Internet.

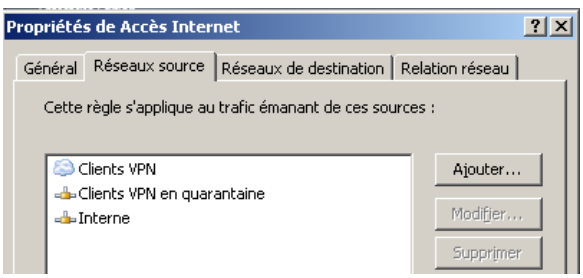
6.1.4 Configurer les règles de réseaux :

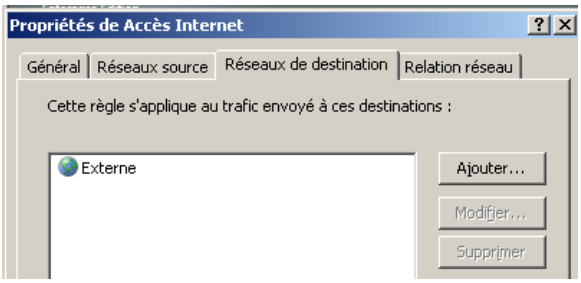
Il faut ensuite vérifier nos règles de réseaux.
Le réseau interne ISA Server dispose d'un réseau interne avec 3 sous réseaux IP en adressage IP privé.
Le réseau externe d'Isa Server 2006 en est en adressage IP publique (Internet).
Il nous faut donc une règle de réseau de type NAT entre le réseau interne et le réseau externe.

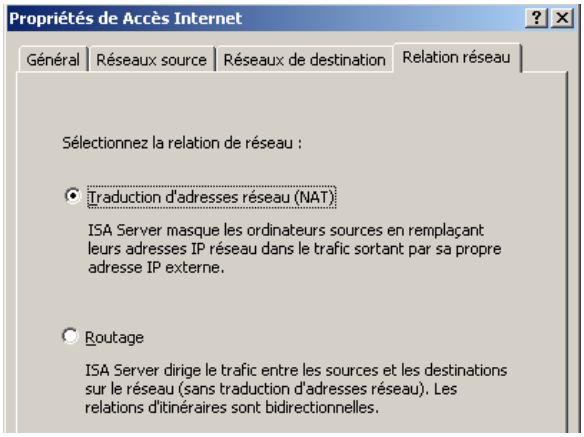
A savoir :

- **Pour qu'une règle d'accès / règle de publication soit analysée, une règle de réseaux doit toujours existée entre le réseau source et le réseau de destination de la règle d'accès / règle de publication.** Si cette règle de réseau n'existe pas, le trafic réseau est refusé par défaut par ISA Server 2006.









Pour plus d'informations sur la configuration des règles de réseaux :

- http://technet.microsoft.com/fr-fr/library/cc302676(en-us).aspx
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part1.html
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part2.html
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part3.html

6.2 Règle d'accès ou règle de publication :

Une fois que l'on a créé les règles de réseaux, il faut créer les règles d'accès et les règles de publication.
Tout d'abord, avant de se lancer dans la configuration d'Isa Server, écrivez vos règles de filtrage sur papier.
Une fois les règles de filtrage écrites sur papier, il faut déterminer si l'on doit créer des règles d'accès ou des règles de publication. Pour cela, voir le tableau ci-dessous.

Relation entre le réseau source et le réseau destination	Sens	Règles ISA
Routage	Entrant ou sortant	Règle d'accès
NAT	Sortant	Règle d'accès
NAT	Entrant	Règle de publication

Remarque sur le sens :
Cas 1 :

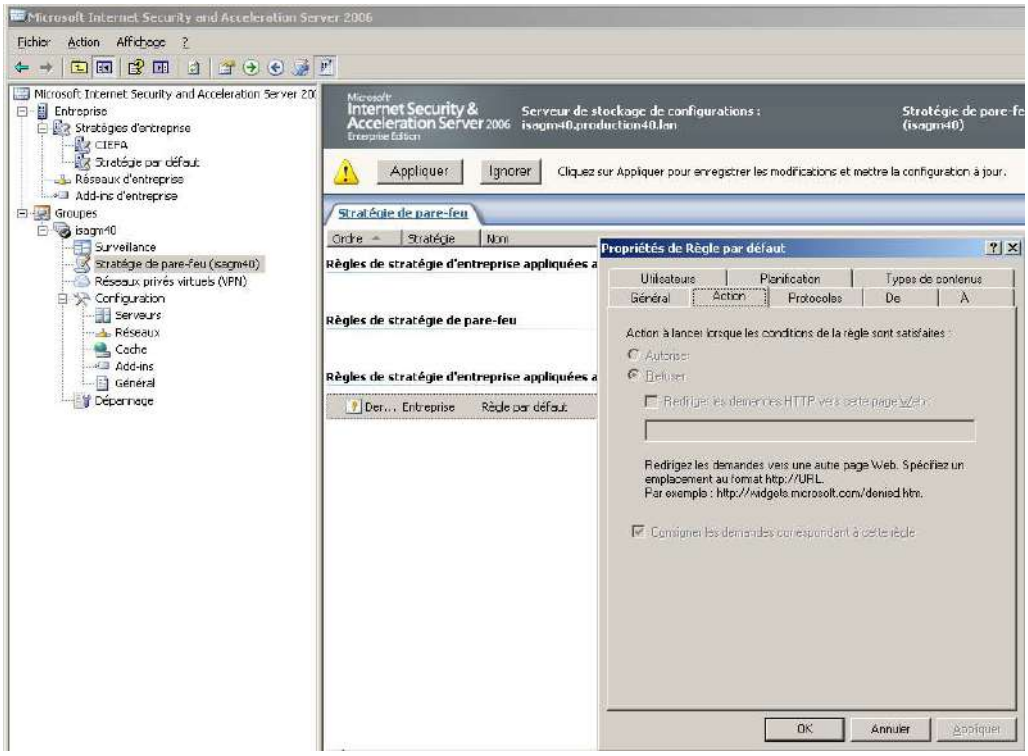
- Source : réseau avec adresse IP privé
- Destination : réseau avec adresse publique
- Sens : sortant

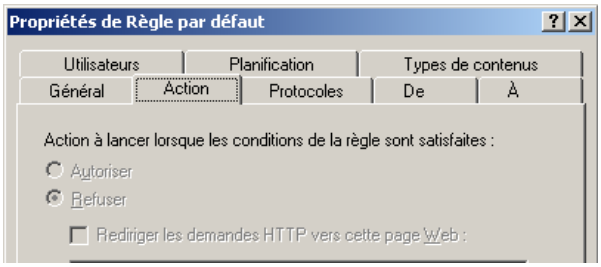
Cas 2 :

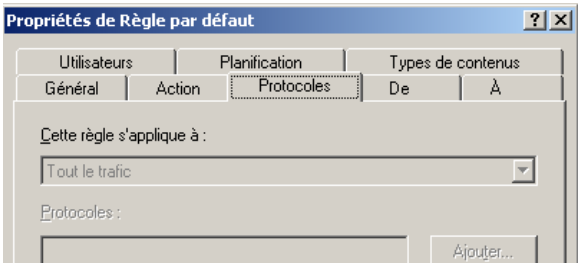
- Source : réseau avec adresse publique
- Destination : réseau avec adresse IP privé
- Sens : entrant

6.3 Les accès par défaut au niveau du serveur Isa Server 2006 :

Par défaut, Isa Server bloque tout le trafic réseau. Il existe en effet une règle par défaut qui interdit tout le trafic réseau.

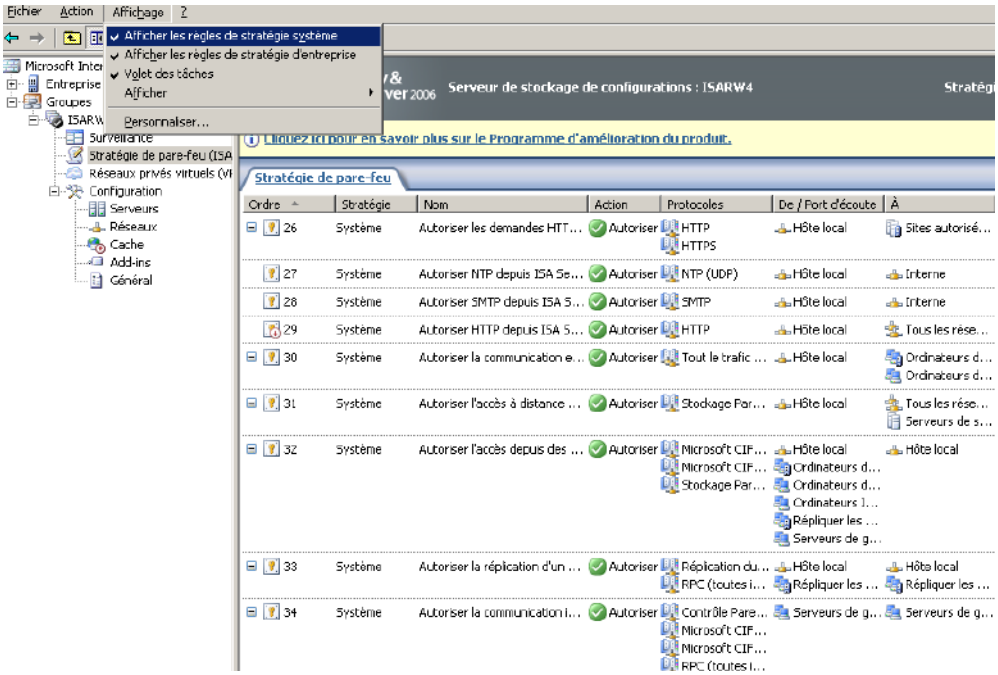






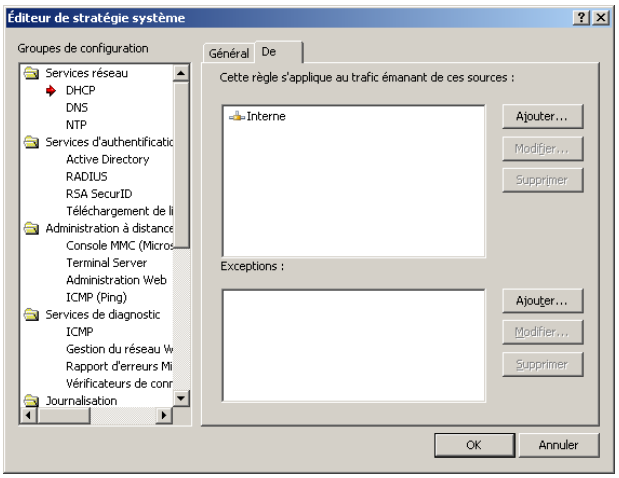
6.4 Les stratégies systèmes :

Par défaut, Isa Server 2006 crée des règles de stratégie système pour filtrer les accès vers et depuis le réseau Hôte Local (Isa Server).
Pour afficher ces règles, cliquer sur le menu « *Affichage* » puis « *Afficher les règles de stratégie système* ».

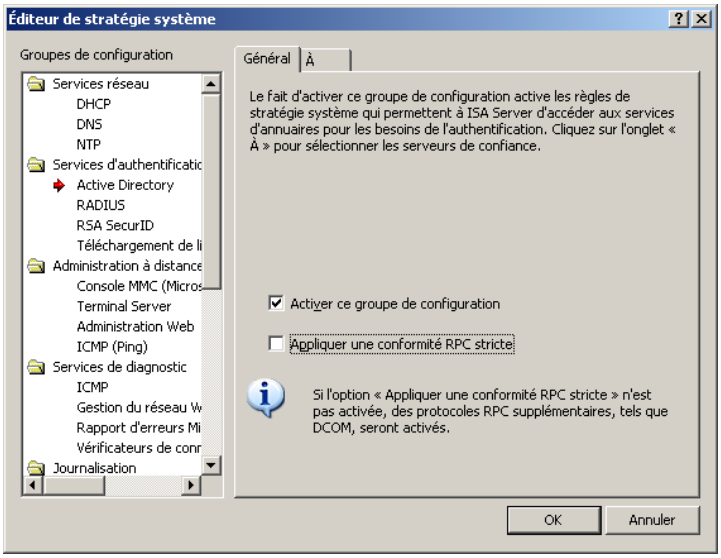


Ces règles peuvent être modifiées.

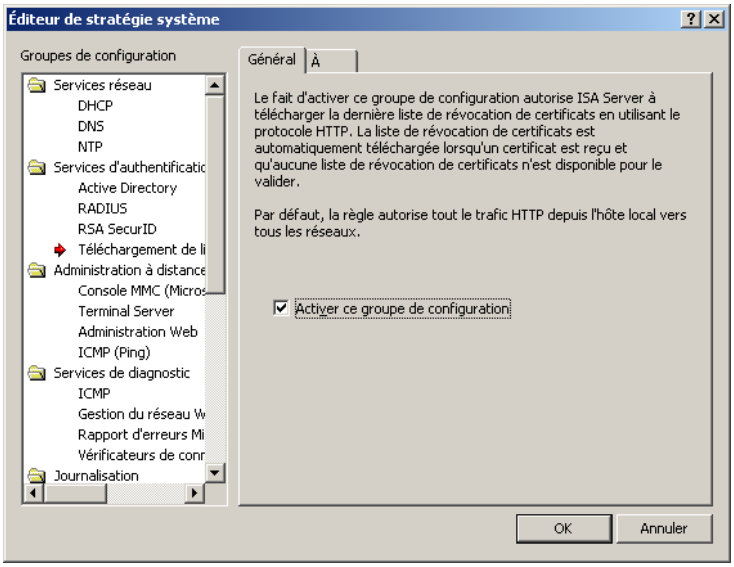
Isa Server 2006 a besoin d'un serveur DHCP pour attribuer des IP aux clients VPN.
Le premier paramètre de la stratégie système va permettre de déterminer quels sont les serveurs DHCP qu'Isa Server peut utiliser.



Le paramètre ci-dessous permet d'autoriser Isa Server à se connecter au domaine.
Décocher la case « *Appliquer une conformité RPC stricte* ».



Le paramètre ci-dessous permet de configurer Isa Server pour télécharger les dernières listes de révocation de certificats (CRL).



Pour plus d'informations sur les stratégies systèmes :

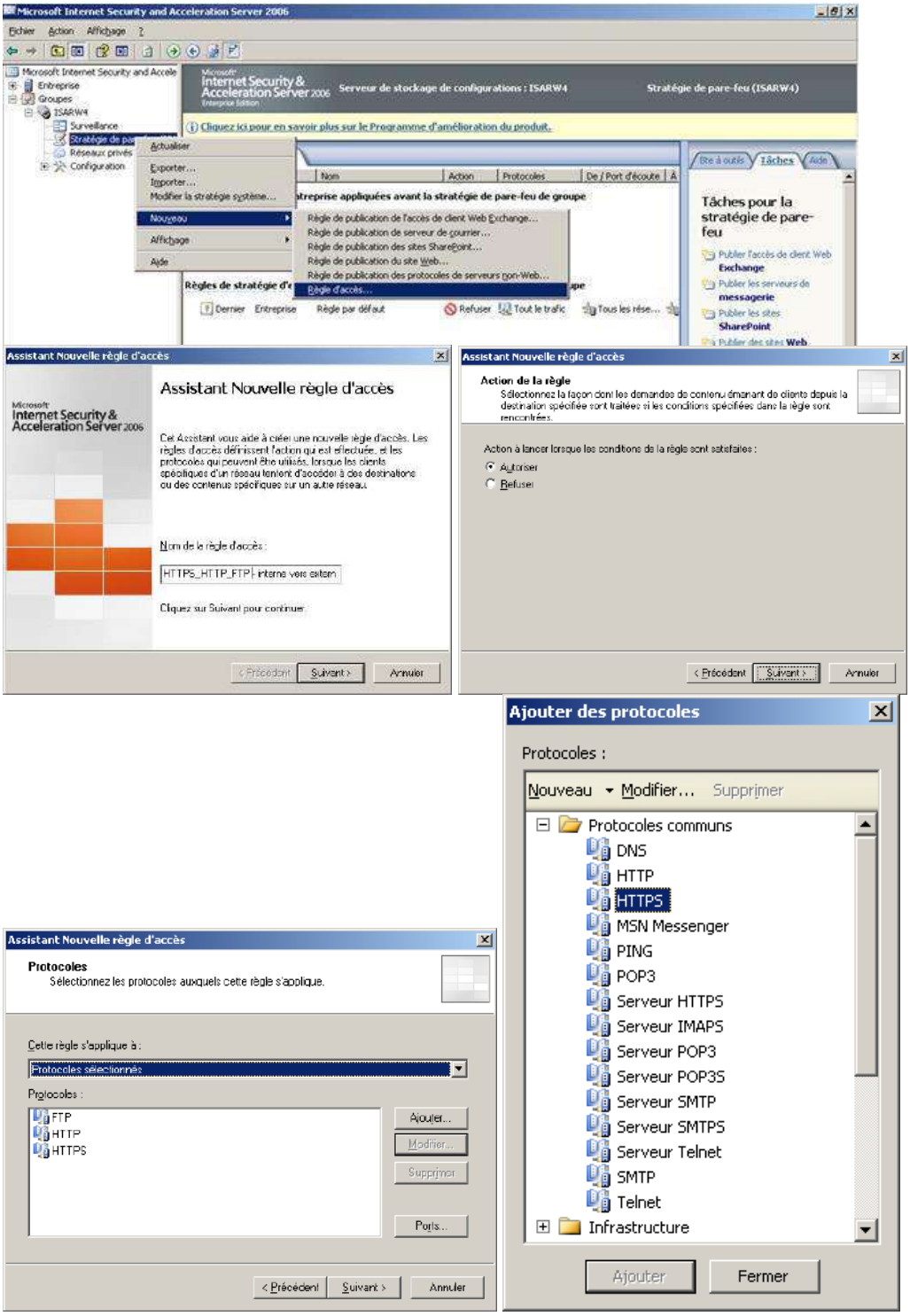
- http://technet.microsoft.com/en-us/library/bb794729.aspx

6.5 Création de règle d'accès :

Les règles d'accès permettent de filtrer :

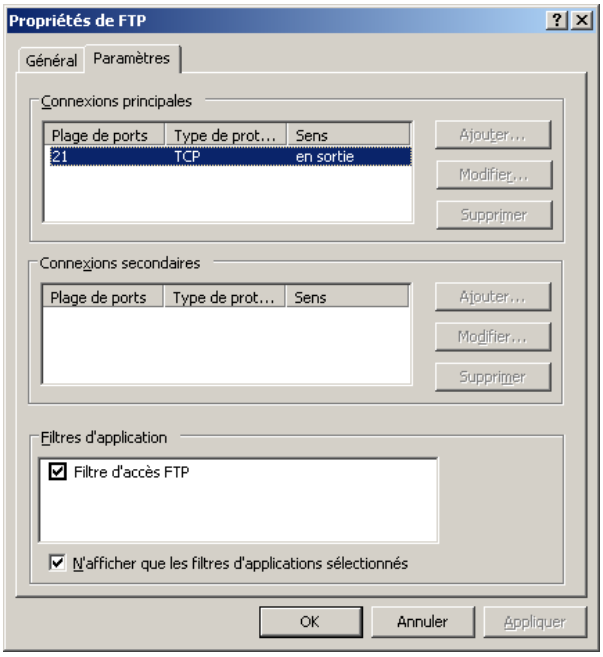
- Sur l'adresse IP source / destination, sur une URL (champs De et A).
- Sur un type de protocole (filtrage sur le port source / destination).
- Sur une plage horaire.
- Sur un ensemble d'utilisateurs.
- Sur les éléments de la couche 7 du modèle OSI (filtrage applicatif).
- Les types de contenus.

Une règle d'accès peut autoriser ou interdire le trafic.

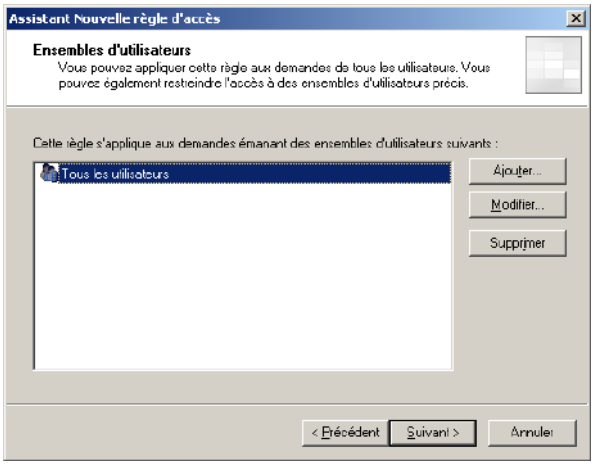


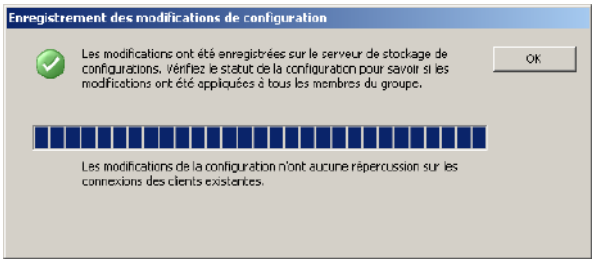
Attention les définitions de protocoles ont un sens.
Pour autoriser en sortie le protocole HTTPS, il faut sélectionner la définition de protocole HTTPS (sens en sortie) et non la définition de protocole Serveur HTTPS (sens : en entrée).

Exemple avec le protocole FTP :



Il faut ensuite spécifier la source (réseau interne) et la destination (réseau externe).
Dans notre cas, nous ne filtrons pas sur les ensembles d'utilisateurs. Il faut donc sélectionner « Tous les utilisateurs » (à la place de « *Tous les utilisateurs authentifiés* »).





Une fois la règle créée, il faut cliquer sur « *Appliquer* » pour qu'elle soit prise en compte.

6.6 Les règles de publication :

Il existe deux grands types de règle de publication :

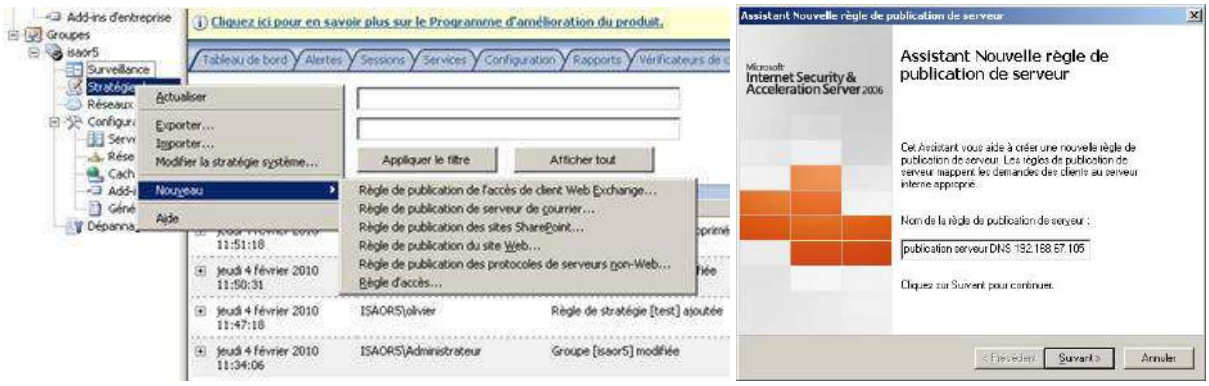
- Les règles de publication de site web. C'est le moteur proxy d'Isa Server 2006 qui gère ce type de règles.
- Les règles de publication de protocoles de serveur non web. C'est le moteur NAT d'Isa Server qui gère ce type de règles.

Remarque :

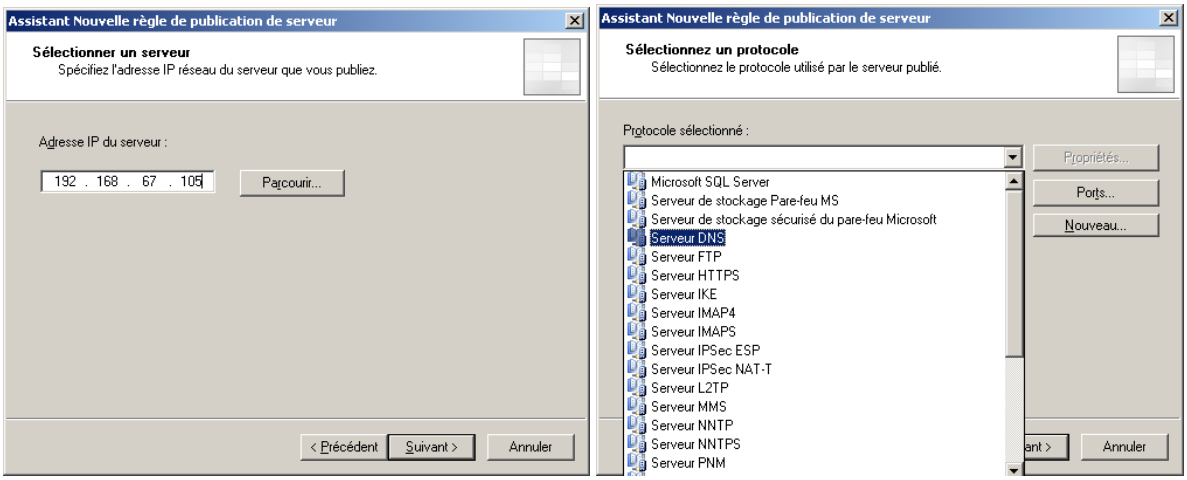
- La règle de publication de l'accès de client web Exchange est une règle de publication du site web préconfigurée pour l'accès Outlook Web Access, ActiveSync et RPC over HTTPS. Cette règle permet de prédéfinir les répertoires virtuelles Exchange à publier entre autres.
- Pour plus d'informations sur les règles de publication : http://technet.microsoft.com/en-us/library/bb794758.aspx

6.6.1 Création d'une règle de publication de serveur non web :

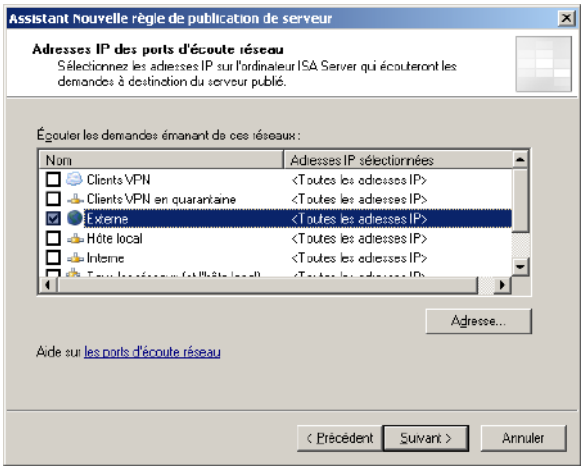
Dans l'exemple ci-dessous, on va publier un serveur DNS situé sur le réseau interne 192.168.67.105. Comme il s'agit d'une règle de publication des protocoles de serveurs non web, c'est le moteur NAT d'Isa Server qui est utilisé. Il faut donc configurer le serveur DNS pour être client Secure NAT ;
Pour cela, configurer le serveur DNS avec comme passerelle le serveur ISA (192.168.67.254).



On rentre l'adresse IP de notre serveur DNS.
Il est possible de filtrer la connexion selon le port source ou de changer le port destination en cliquant sur l'onglet Ports.
En effet, Isa Server permet de configurer une règle qui permet de se connecter sur la patte externe du serveur Isa sur le port TCP 53 et de rediriger le trafic sur un serveur interne sur le port TCP 54 (Isa fait du *Port Translation Address* ou PAT). Dans notre cas il faudrait cependant reconfigurer le serveur DNS interne pour écouter les demandes sur le port TCP 54 au lieu du port TCP 53.



Il faut autoriser les demandes depuis le réseau externe. Le but est que notre serveur DNS soit accessible depuis Internet.



Depuis Internet, il est maintenant possible de se connecter au serveur DNS en se connectant sur le port TCP 53 sur l'IP de la carte réseau externe du serveur ISA.

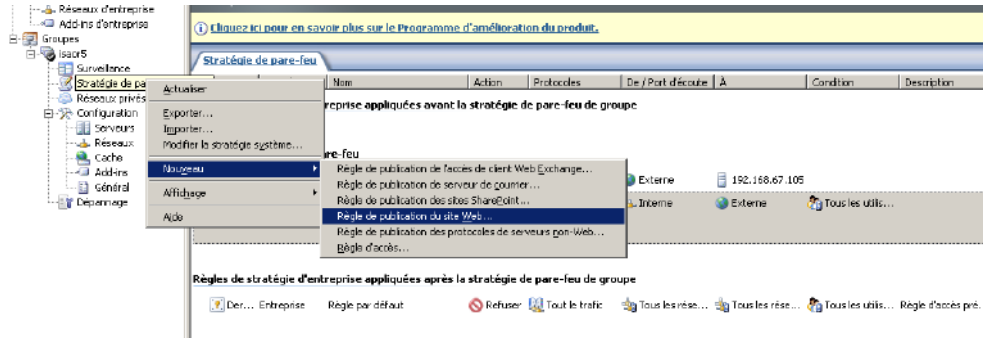
Dans notre cas il faut faire un *TELNET 193.252.19.1 53*

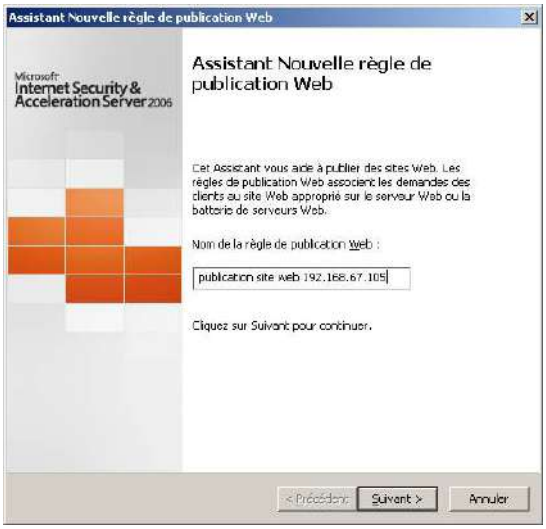
6.6.2 Les règles de publication de serveur web :

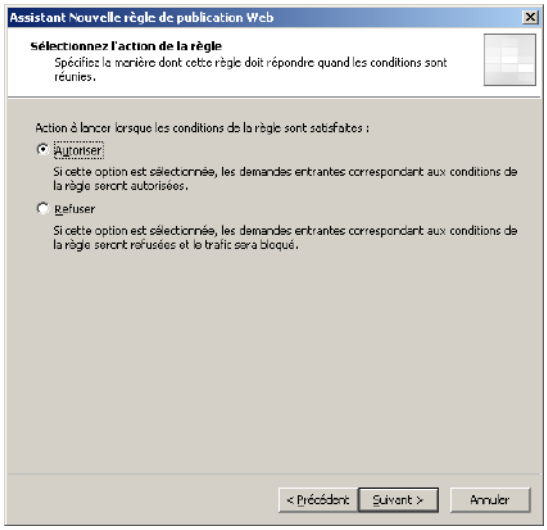
On va maintenant voir comment publier un serveur web HTTP.
Tout d'abord, il faut comprendre que ce type de règle passe par le moteur proxy d'Isa Server 2006.
Isa Server 2006 va donc jouer le rôle de mandataire.
Quand un utilisateur externe (sur Internet) se connecte sur un serveur web interne publié avec Isa Server 2006, deux sessions sont établies :

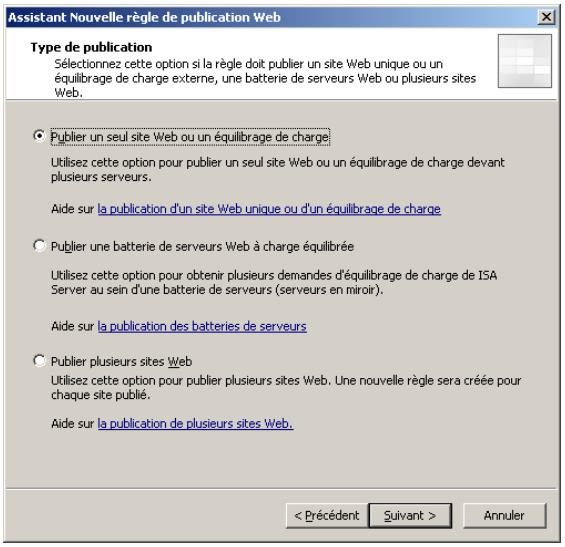
- La première session est entre le client Internet et le serveur Isa.
- La seconde session est entre le serveur Isa et le serveur web interne.

Dans le langage Isa Server, on parle de pontage HTTP / HTTP.



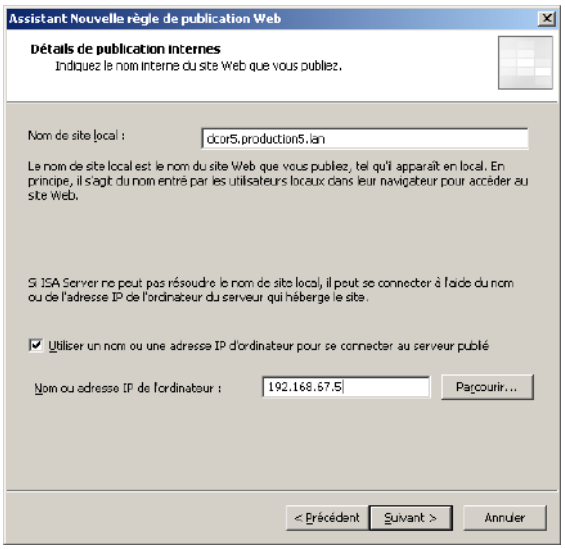


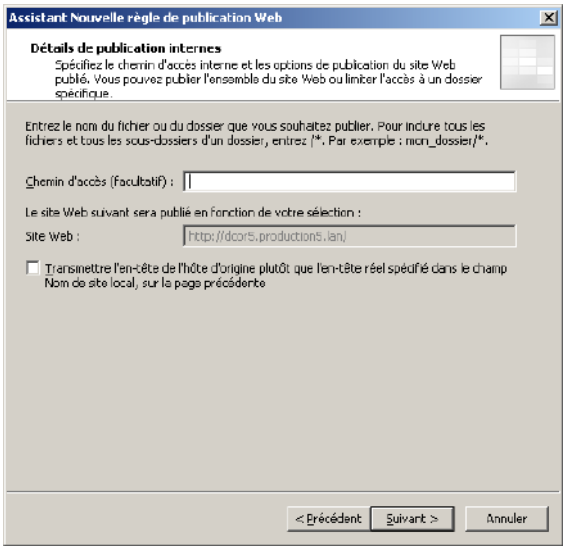




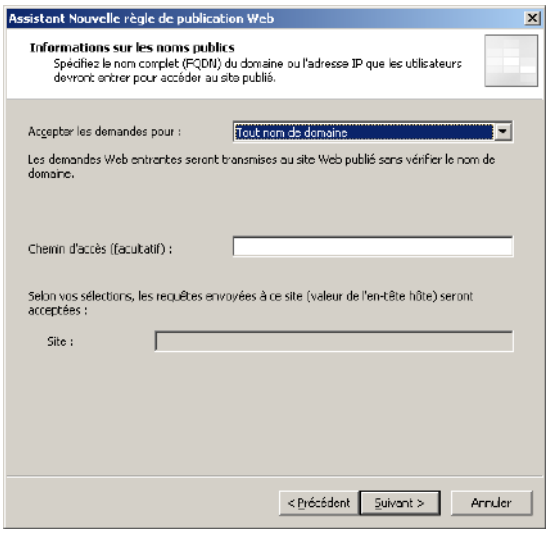
La première partie de règle permet de configurer la session entre Isa Server et le serveur web interne.
Attention dans le cas d'une règle de publication HTTPS – HTTPS (pntage SSL), il faut que le nom du serveur interne soit le même que celui contenu dans le certificat du serveur web interne.

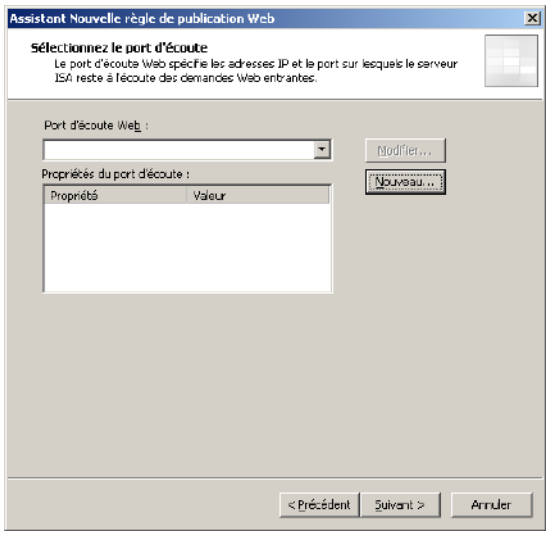
Il est possible de publier qu'une partie d'un site web (un répertoire virtuel).
Pour publier uniquement le répertoire virtuel OWA, mettre /**owa/***
Ne pas oublier le /*. Dans le cas contraire la règle de publication ne fonctionnera pas.

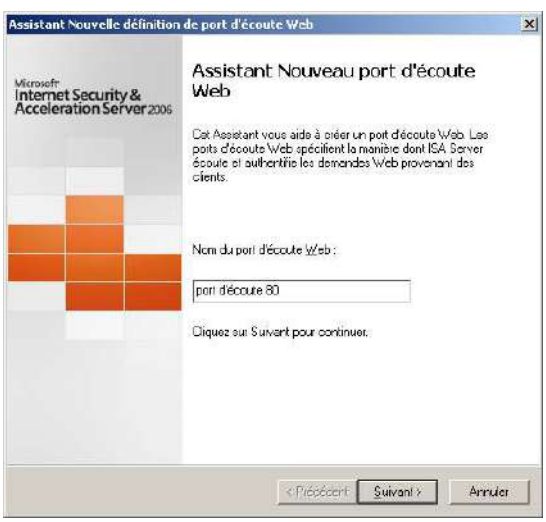




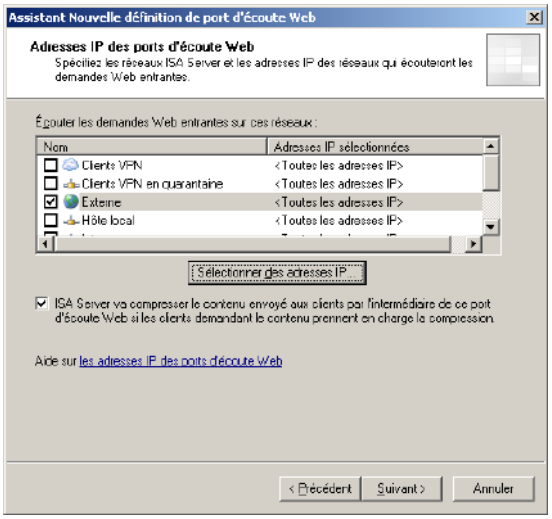
La suite de la règle nous permet de configurer la session entre le client web et le serveur ISA Server 2006.
Il est possible comme avec IIS de filtrer selon le nom DNS (en tête d'hôte).
Dans notre cas, nous configurons la règle pour accepter les connexions avec tout nom de domaine.
Il faut ensuite créer un port d'écoute pour configurer les paramètres d'authentification et l'adresse IP externe / le port d'écoute du serveur Isa Server.

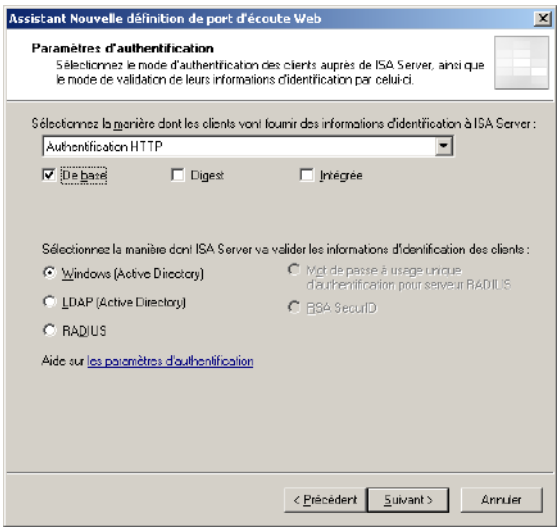


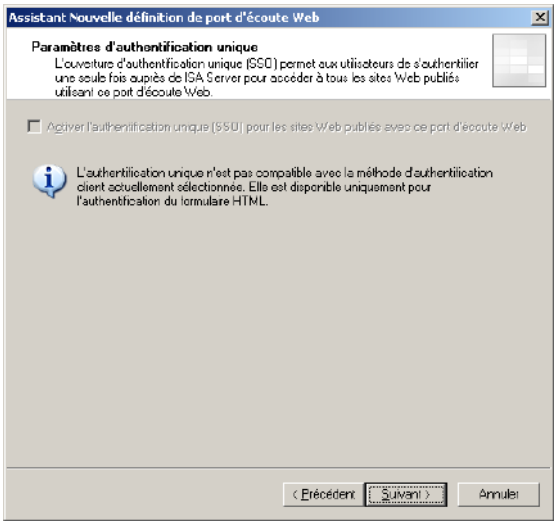


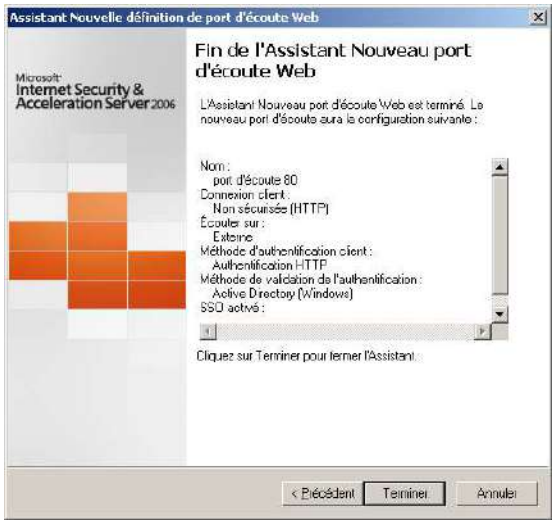


Dans notre cas, le serveur Isa Server 2006 dispose d'une seule adresse IP publique.
Si le serveur Isa Server 2006 dispose de plusieurs adresses IP publiques, il est possible de publier le site web que sur cette IP.
Il faut ensuite sélectionner le protocole d'authentification correspondant.
Isa Server 2006 permet par exemple une authentification par formulaire.

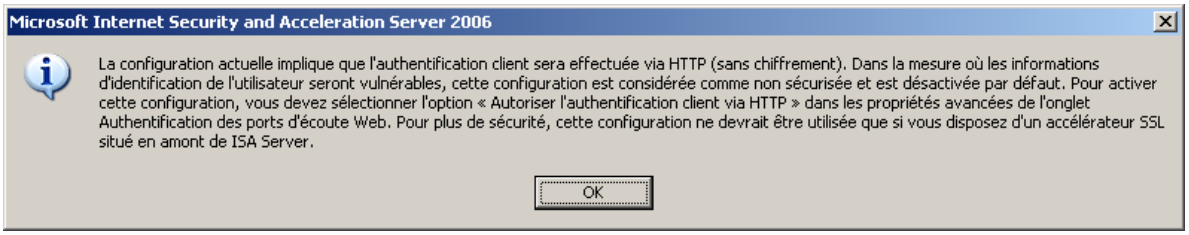




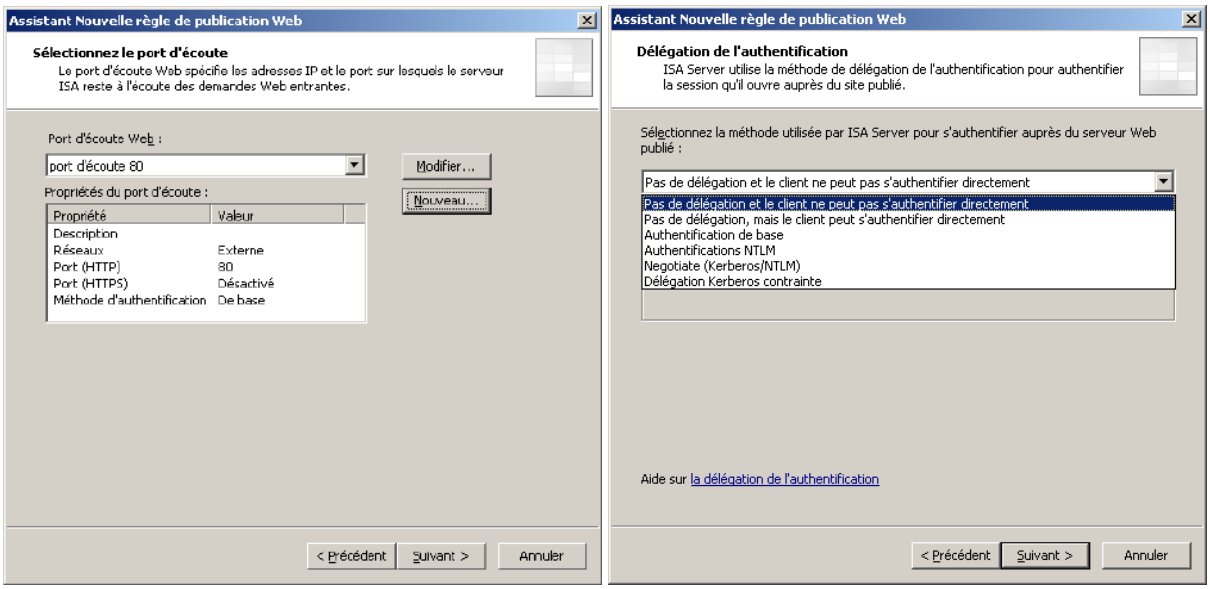




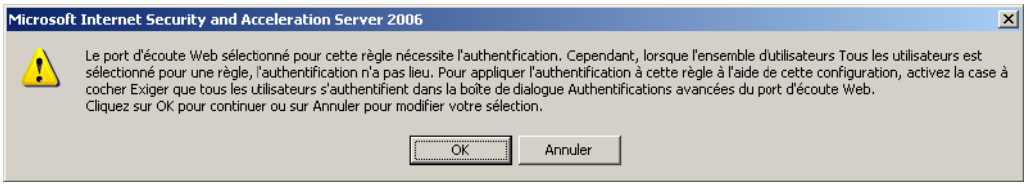
Le message ci-dessous s'affiche car on va faire de l'authentification en HTTP. Le mot de passe de l'utilisateur va donc passer en clair via Internet. Cela n'est très clairement pas à faire en production. Il faudra passer en HTTPS.



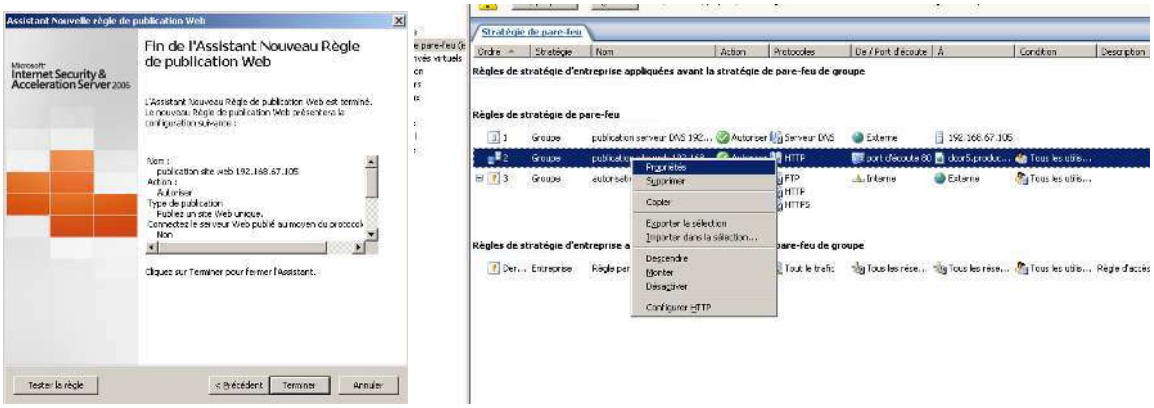
Sélectionner le port d'écoute web que l'on vient de créer.
La capture de droite permet ensuite de définir comment Isa Server 2006 va se connecter au serveur web interne.
Dans notre cas, on sélectionne « *Authentification de base* » (contrairement à ce qui est indiqué sur la capture).

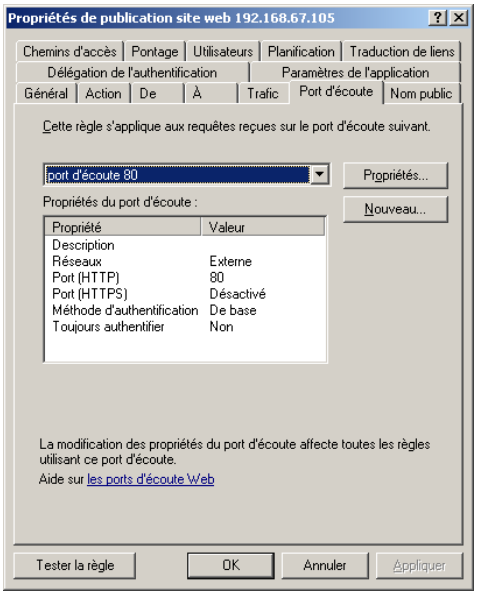


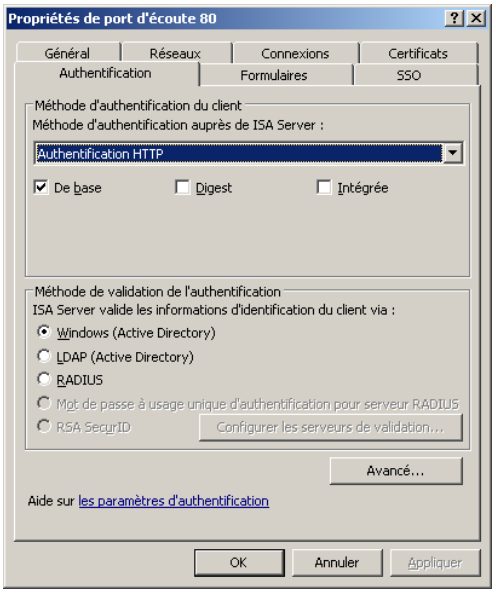
Sélectionner ensuite « *Tous les utilisateurs* ». Ce mode de configuration va faire que seul le serveur web interne demandera l'authentification (on évite d'avoir deux POPUP d'authentification). On peut aussi utiliser les nouvelles méthodes de « *Délégation Kerberos contrainte* » pour éviter la double authentification.

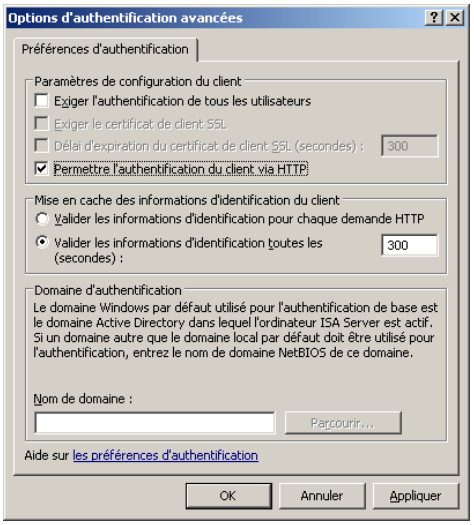


Cliquer sur Terminer puis aller dans les propriétés de la règle.
Par défaut Isa Server 2006 bloque l'authentification HTTP. Il faut donc aller modifier le port d'écoute et cocher la case « *Permettre l'authentification du client via HTTP* ».

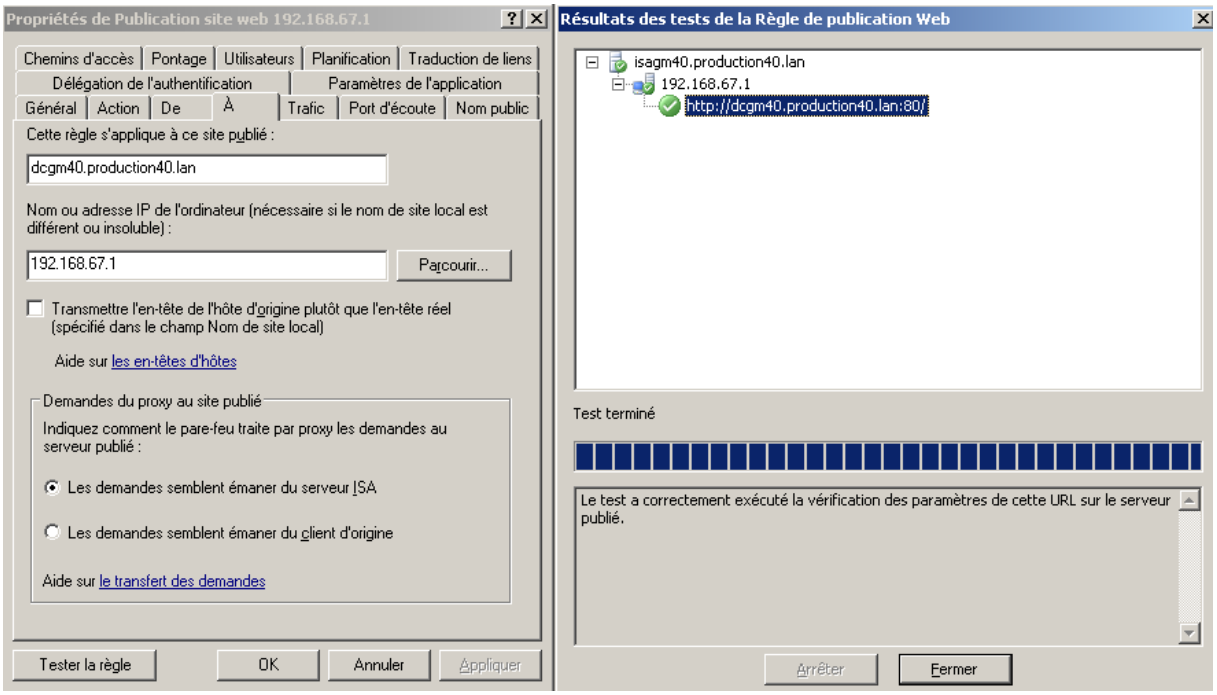








On peut maintenant appliquer la règle et la tester (nouveauté du SP1).



6.6.3 Configuration des règles de publication web HTTPS et des règles pour publier Outlook Web Access, ActiveSync et Outlook Anywhere :

De nombreux site web expliquent comment publier un site web via un pontage SSL (deux connexions HTTPS) :

- http://www.isaserver.org/tutorials/Publishing-Exchange-2007-OWA-Exchange-ActiveSync-RPCHTTP-2006-ISA-Firewall-Part6.html
- http://technet.microsoft.com/en-us/library/bb794751.aspx
- http://technet.microsoft.com/fr-fr/library/aa998934(EXCHG.80).aspx
- http://technet.microsoft.com/fr-fr/library/bb201695(EXCHG.80).aspx
- http://www.msexchange.org/tutorials/Outlook-Anywhere-2007-ISA-Server-2006.html

Si votre client est en train de migrer d'Exchange 2003 vers Exchange 2007, appliquer la procédure suivante pour publier Outlook Web Access et ActiveSync du serveur Exchange 2003 et Exchange 2007 avec le même serveur ISA et une seule adresse IP publique :

- http://msreport.free.fr/?p=164

6.7 Configuration de la mise en cache avec Isa Server 2006 :

Isa Server 2006 permet de mettre en cache le contenu des sites web HTTP, HTTPS et FTP.
Par défaut la mise en cache avec Isa Server 2006 est désactivée.
Les administrateurs des sites web peuvent spécifier les paramètres de mise en cache de leurs sites web à l'aide des balises META. Pour plus d'informations, voir :
http://www.commentcamarche.net/forum/affich-17721-balise-meta
Si le site web change très souvent de contenu, la mise en cache peut être problématique et doit donc être désactivée. L'administrateur du site web renseigne alors la balise META dans ce sens.
Isa Server permet de d'activer / désactiver / configurer la mise en cache des sites web et FTP à l'aide :

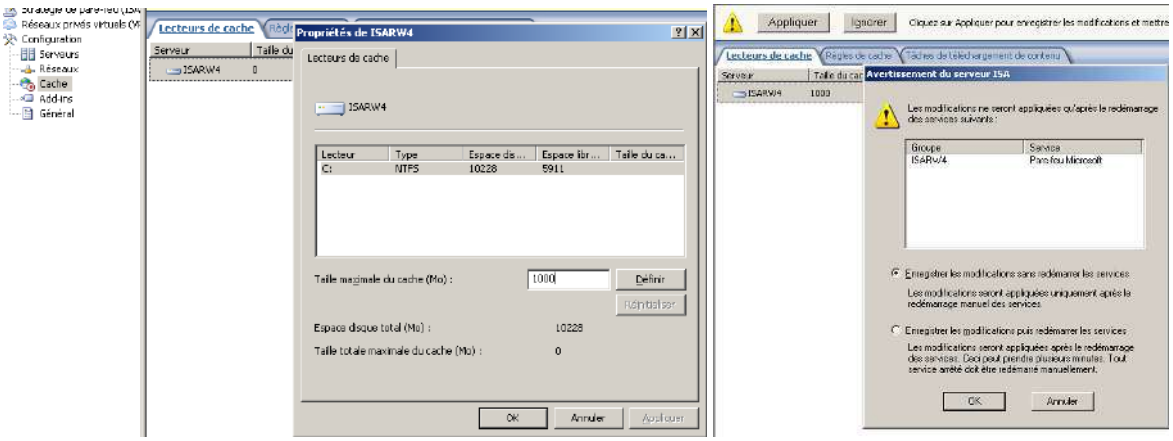
- Des règles de cache.
- Des règles de téléchargement planifiées.

Pour plus d'informations :

- http://www.isaserver.org/tutorials/ISA-Firewall-Web-Caching-Capabilities.html
- http://www.isaserver.org/tutorials/Understanding-Web-Caching-Concepts-ISA-Firewall.html
- http://www.isaserver.org/tutorials/ISA-2006-Web-Caching.html

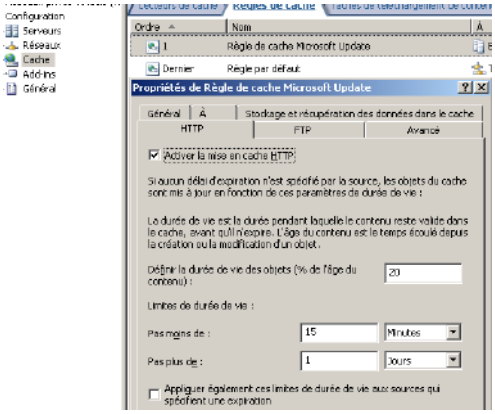
6.7.1 Activer le cache sur le serveur Isa Server 2006 :

Tout d'abord, il est nécessaire d'activer le cache Isa Server 2006. Pour cela, appliquer la procédure ci-dessous. Il est alors nécessaire de redémarrer le service pare feu (attention arrêt de production).



6.7.2 Configurer les règles de cache :

Il est ensuite possible de configurer les règles de cache pour empêcher la mise en cache de certains sites web ou de modifier les paramètres par défaut de la mise en cache.

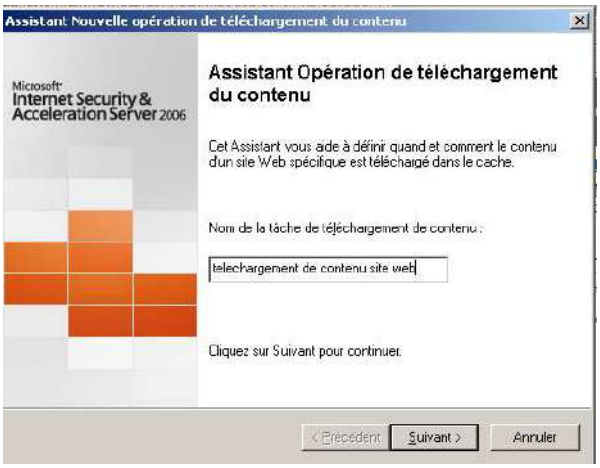


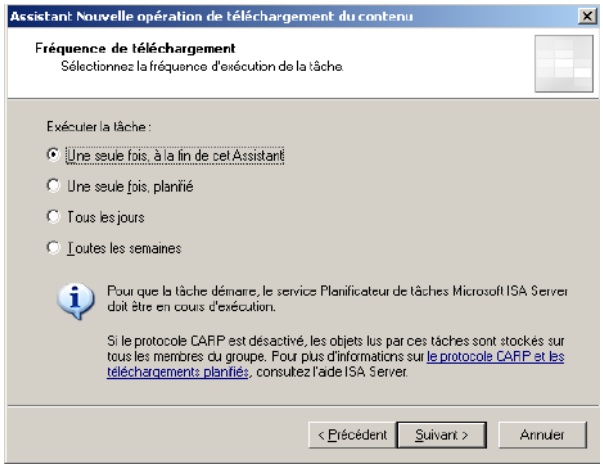
La mise en cache FTP est configuré par exemple sur 1 journée ce qui peut être problématique dans certains cas.

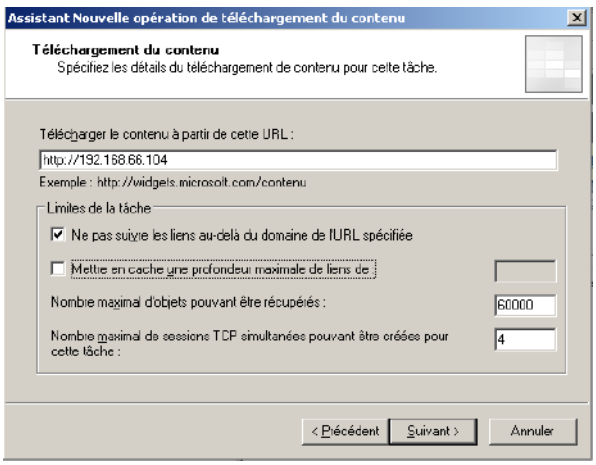
6.7.3 Création de tâches de téléchargement de contenu :

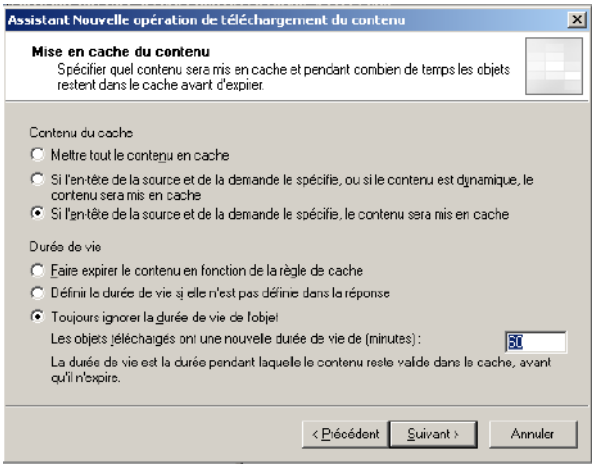
Isa Server permet de télécharger le contenu de site web en heure creuse afin d'accélérer la navigation en heure pleine.

Pour que la règle de téléchargement planifiée fonctionne, il faut autoriser le serveur Isa Server à accéder au site web et donc modifier la stratégie système.









6.7.4 Gestion du contenu du cache :

L'utilitaire *Cache Directory Tool for Internet Security and Acceleration (ISA) Server 2006* permet de gérer le contenu du cache et de marquer une page en cache comme expirée.
Pour plus d'informations sur cet outil, voir :

- http://www.microsoft.com/downloads/details.aspx?familyid=b9ecfcd3-c13f-4447-83ed-add9a8ea45db&displaylang=en

6.8 Configuration de la découverte automatique :

Isa Server peut être configuré pour permettre au client proxy web et pare feu de découvrir automatiquement le serveur Isa Server. Pour plus d'informations, voir :

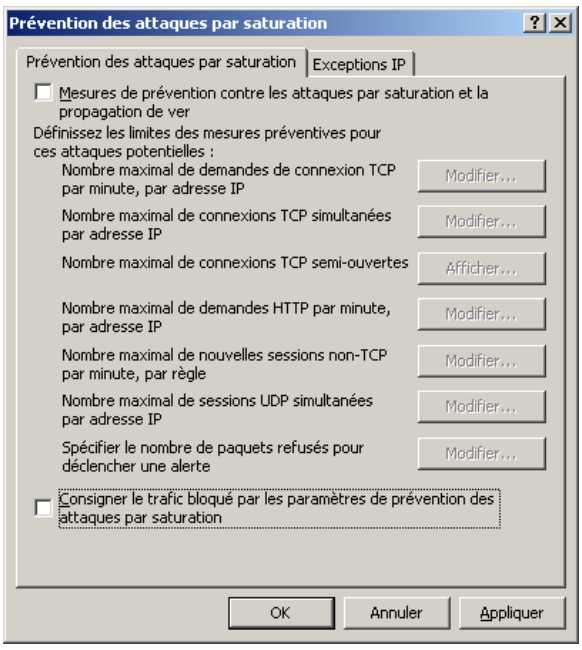
- http://www.isaserver.org/tutorials/Configuring-WPAD-Support-ISA-Firewall-Web-Proxy-Firewall-Clients.html

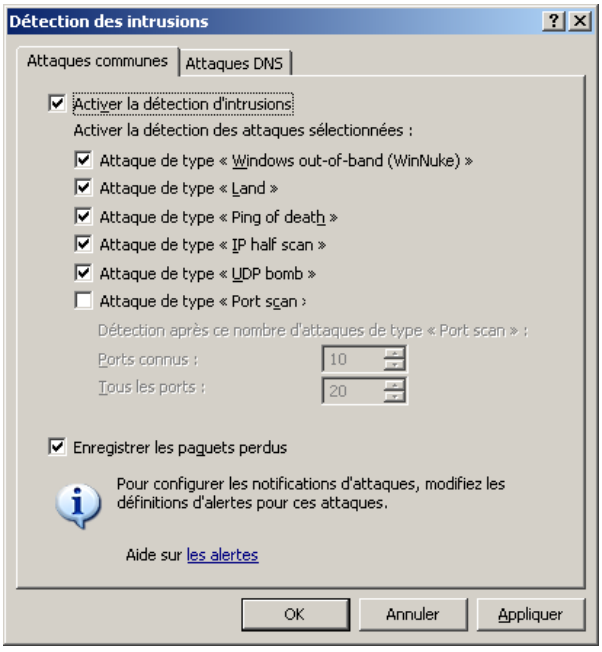
6.9 Configuration de la détection d'intrusion :

Isa Server intègre des outils (très limité) dé détection et de prévention d'intrusion.
Très clairement, je préconise de désactiver les mesures de prévention contre les attaques par saturation. En effet, rien n'empêche un attaquant de générer des très nombreuses trames en usurpant l'IP d'une partenaire de la société. Hors dans ce cas les « mesures de prévention contre les attaques par saturation » risque de faire plus de mal qu'autres choses (bloquer du trafic légitime d'une entreprise partenaire de la votre…).

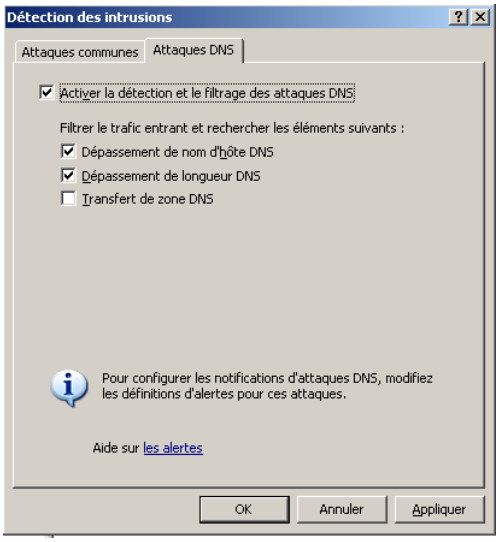
Dans tous les cas préférer loguer les attaques et éviter de couper le flux automatiquement en cas de détection d'attaque.

Le module IDS d'Isa Server 2006 gère surtout d'ancienne attaque qui sont maintenant nativement géré par les piles TCP/IP modernes. Un des modules intéressant dans l'IDS est la détection des attaques DNS.



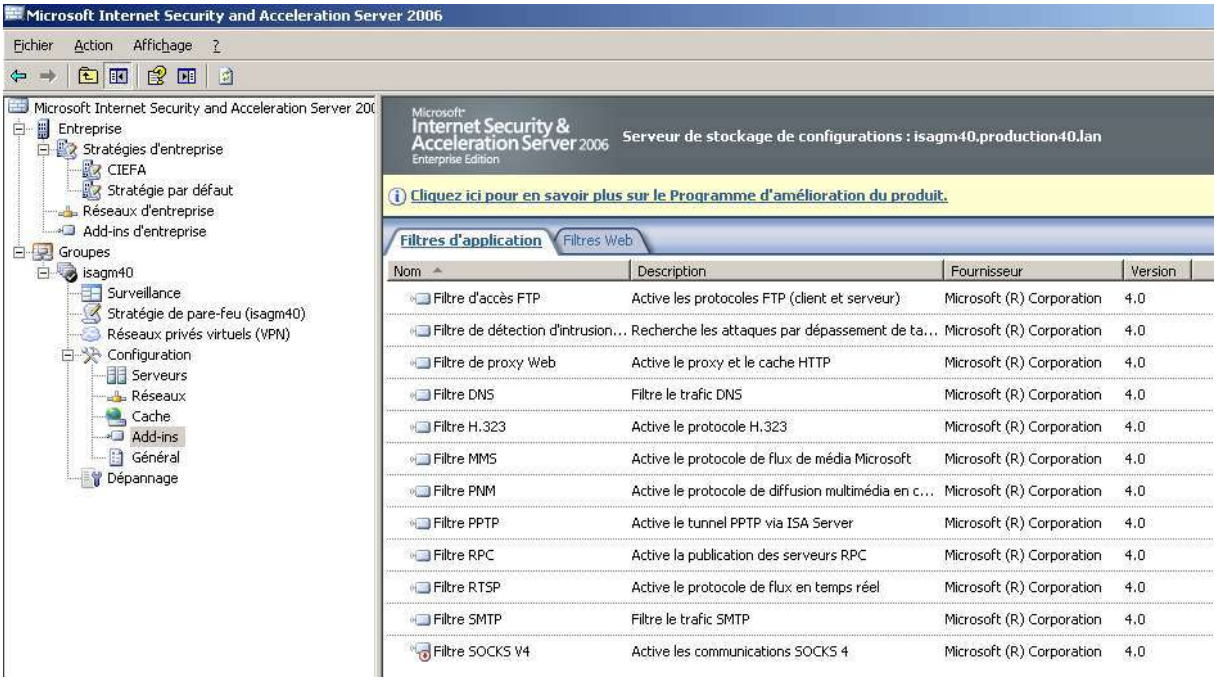


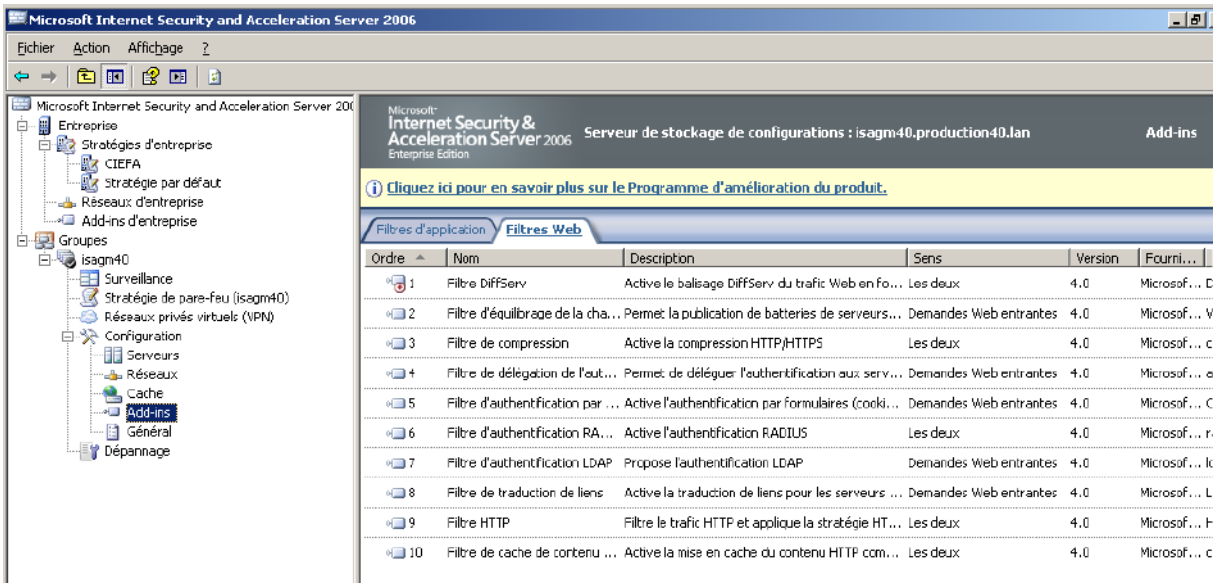
.



6.10 Mise en œuvre du filtrage applicatif avec Isa Server 2006 :

Le gros point fort d'Isa Server 2006 est sa capacité à effectuer du filtrage au niveau 7 de la couche OSI. On parle dans ce cas de filtrage applicatif.
Isa Server 2006 intègre de nombreux filtre applicatif.
Pour plus d'informations, voir http://technet.microsoft.com/en-us/library/bb794732.aspx



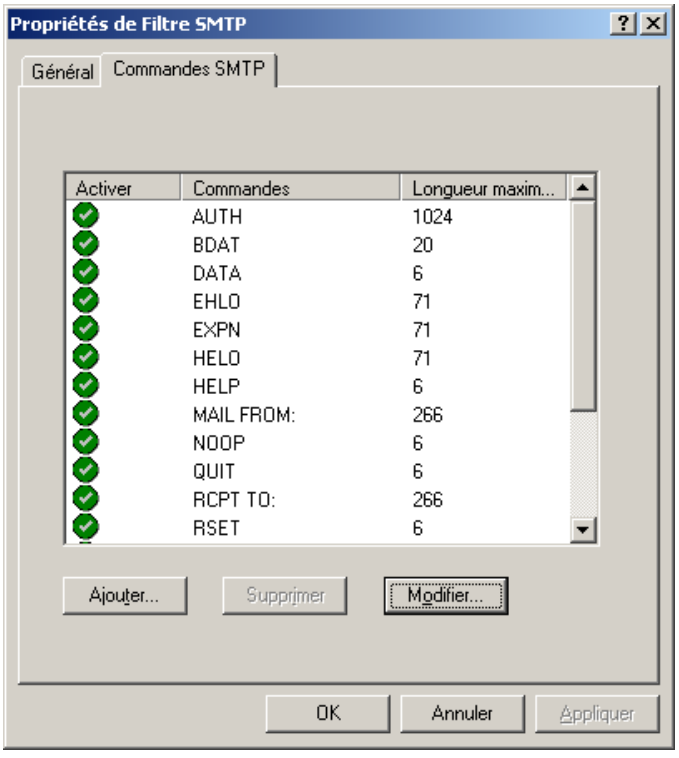


Les filtres applicatifs peuvent être gérés à deux niveaux :

- Au niveau du filtre (cas du filtre SMTP).
- Au niveau d'une règle d'accès (cas du filtre HTTP).

6.10.1 Présentation du filtre applicatif SMTP

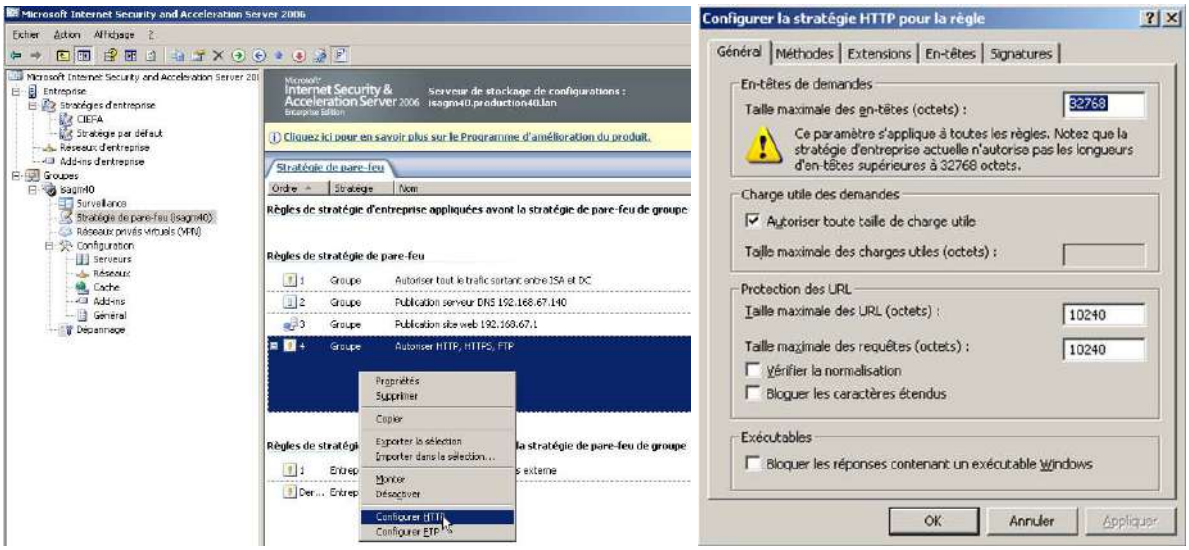
Le filtre SMTP va nous permettre de bloquer certaines méthodes / commandes SMTP qui ne sont pas par exemple utilisés par les serveurs SMTP autorisés.



6.10.2 Présentation du filtre applicatif HTTP :

Le filtre HTTP d'Isa Server 2006 permet de filtrer les trames http :

- Selon la taille de l'entête
- La charge utile des requêtes : une requête GET contient généralement une URL et a donc une taille très faible. Le trafic web est logiquement très asymétrique (on reçoit plus qu'on envoie). Voici une technique très simple pour détecter les tunnels HTTP.
- Selon le type de méthode HTTP (GET, POST…).
- Selon une siganture.



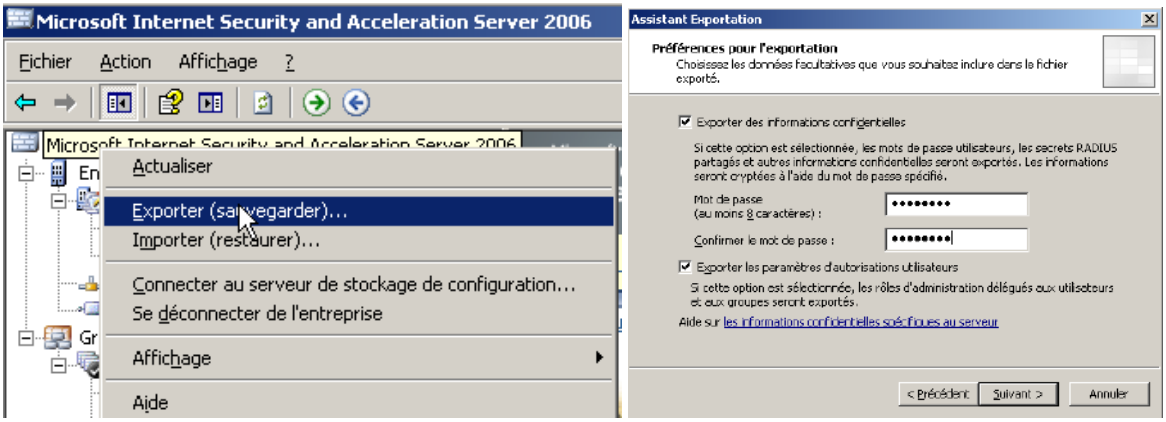
Pour plus d'informations sur le filtre HTTP :

- http://windowsitpro.itpro.fr/Dossiers-par-Theme/suivante/1/8/050382915-1.1-Les-limitations-inherentes-aux-regles-d-acces.htm#R1
- http://www.laboratoire-microsoft.org/articles/server/Filtre-HTTP/3-le-filtre-http/

7 Les tâches d'administration courante d'Isa Server :

7.1 Sauvegarder son serveur Isa Server :

Pour sauvegarder son serveur ISA, on peut exporter toute la configuration.
Pour cela, appliquer la procédure ci-dessous :



Il faut aussi penser à exporter tous les certificats web installés sur le serveur Isa au format PFX (clé publique et clé privée). Pour plus d'informations sur l'exportation de certification, voir :

- http://technet.microsoft.com/fr-fr/library/cc738545(WS.10).aspx

Pour plus d'informations sur la sauvegarde Isa Server, voir :

- http://www.isaserver.org/tutorials/ISA-Server-2006-Backup-Restore-Capabilities.html

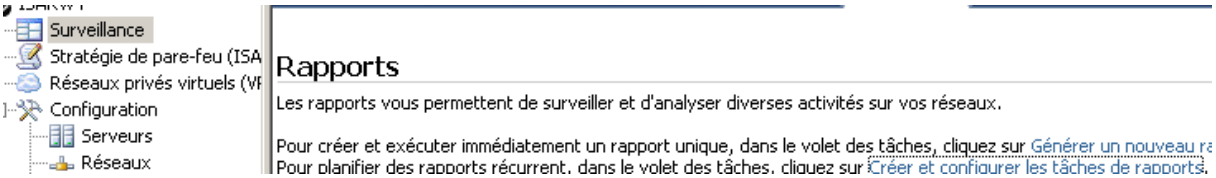
7.2 Mise en œuvre de la délégation d'administration avec Isa Server 2006 :

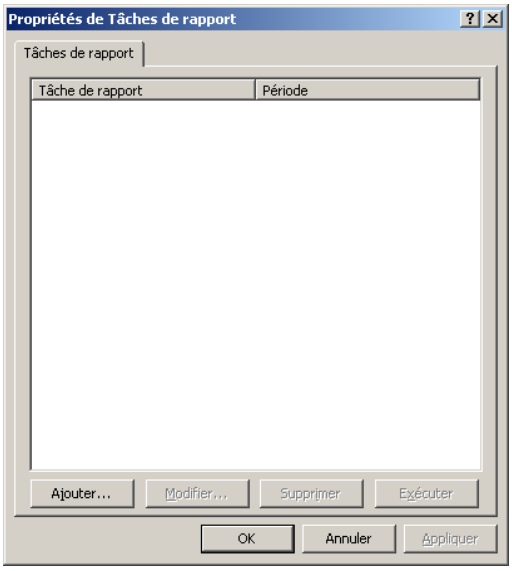
Une Best Practice est de créer des comptes d'administration nominatifs Isa Server et d'activer le suivi des modifications (nécessite installation du SP1 d'Isa Server 2006). Pour plus d'informations :

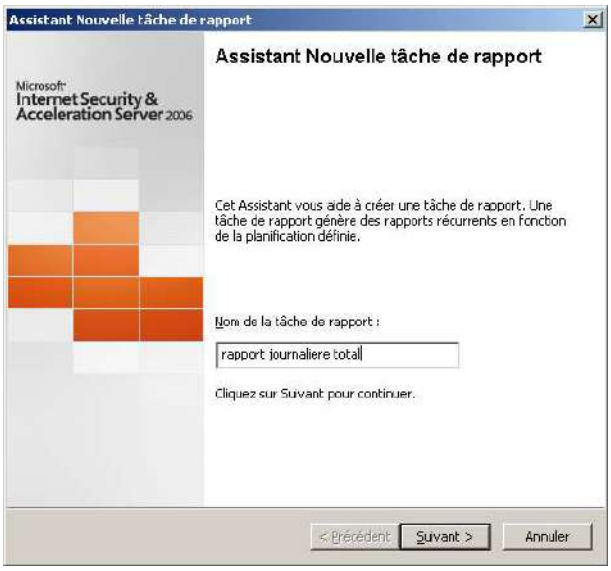
- http://www.isaserver.org/tutorials/Role-based-administration-ISA-Server-2006.html

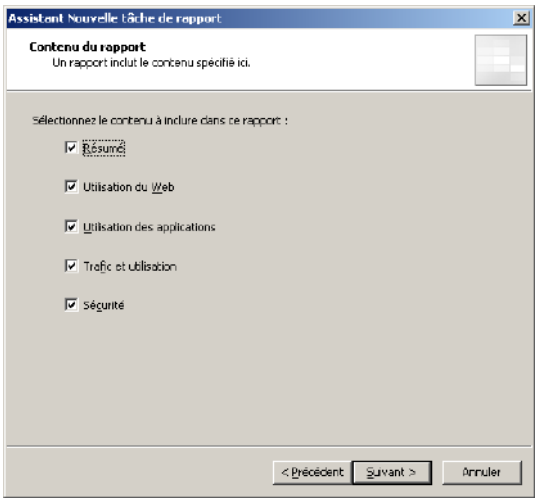
7.3 Configuration de rapports avec Isa Server 2006 :

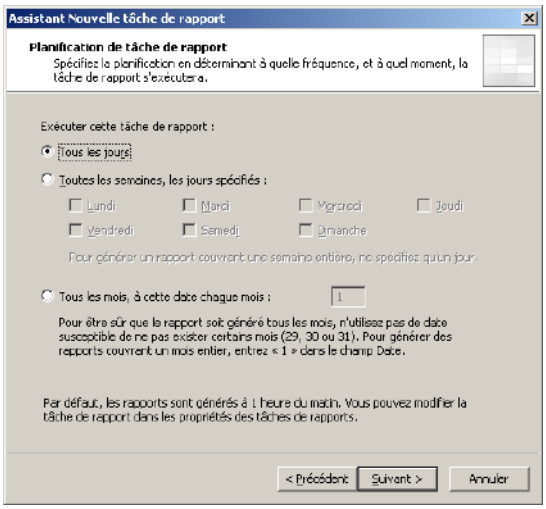
Les rapports permettent de déterminer entre autres comment est utilisée la connexion Internet.
Attention les rapports Isa Server ne peuvent pas être générés pour la journée en cours, seulement pour la veille.
Par défaut, toutes les connexions effectuées à travers Isa Server sont journalisés dans une base de données MSDE (une base pour chaque journée par défaut).

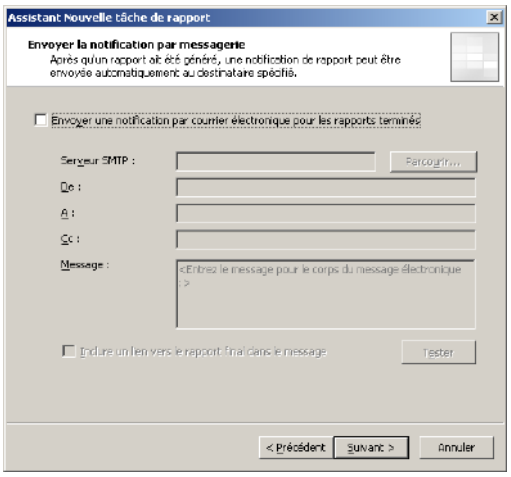










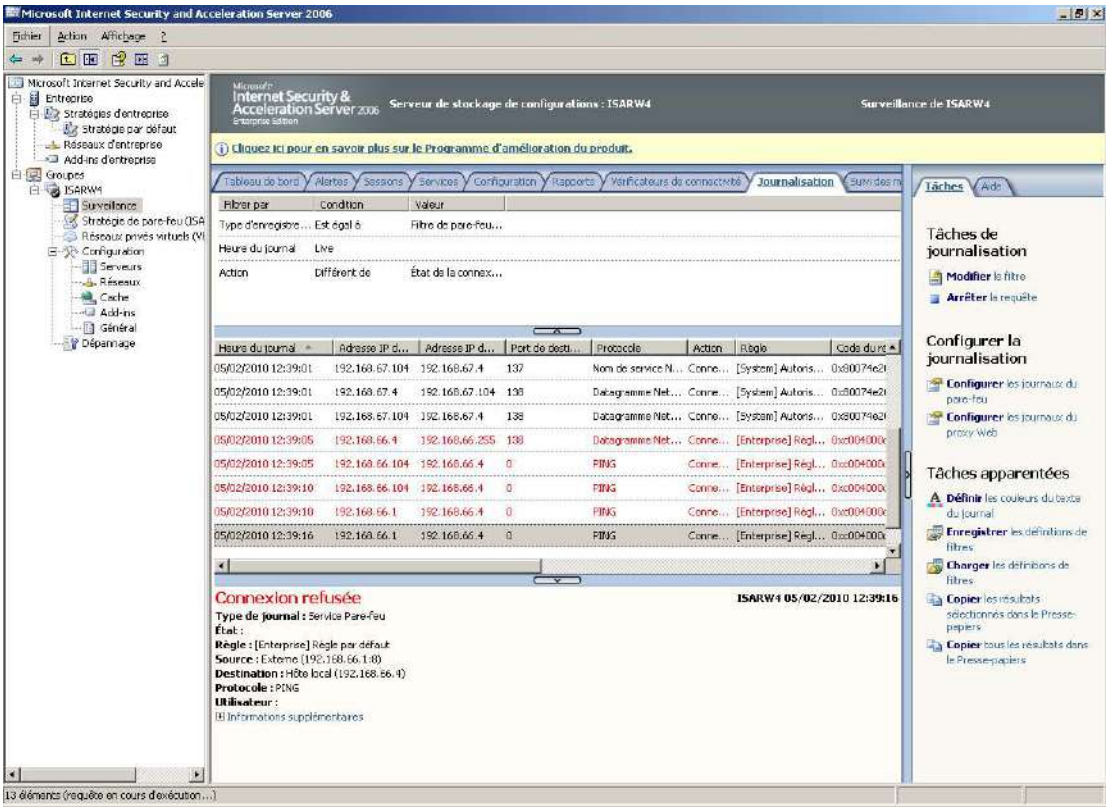


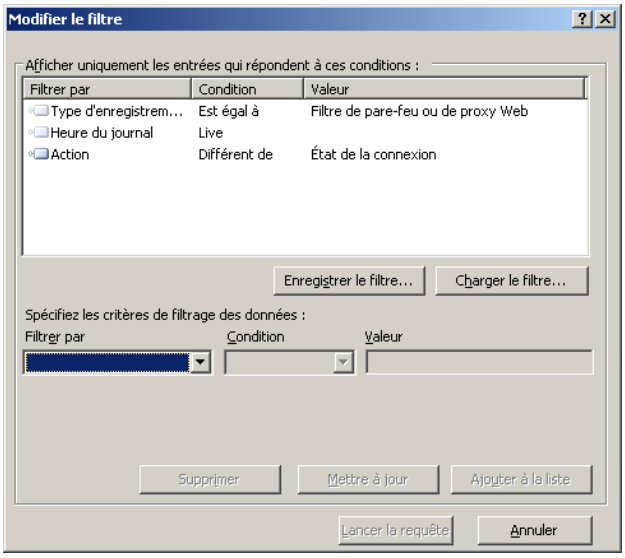
Pour plus d'informations sur la mise en œuvre de rapport avec Isa Server 2006 :

- http://www.isaserver.org/tutorials/Logging-Reporting-ISA-Server-2006.html

7.4 Troubleshouting avec l'onglet Surveillance\Journalisation :

Il est possible de monitoirer toutes les connexions en cours sur le serveur et les filtrer entre autres selon l'adresse IP source / cible.
Pour chaque connexion, il est possible de connaître la règle Isa Server qui s'est appliquée et de savoir si la connexion a été acceptée ou refusée.





8 Mise en œuvre des VPN :

Isa Server 2006 supporte deux types de VPN :
- PPTP
- L2TP

Isa Server ne fait qu'intégrer dans son interface les fonctionnalités du service RRAS de Windows 2003 Server (simplification de l'interface).
Pour plus d'informations sur la prise en charge des VPN par Isa Server 2006 :
- http://technet.microsoft.com/en-us/library/bb794723.aspx

8.1.1 Configuration d'Isa Server comme serveur VPN L2TP :

Appliquer la procédure ci-dessous :
- http://www.laboratoire-microsoft.org/articles/server/ISA2004/6/

Pour plus d'informations :
- http://www.isaserver.org/tutorials/2004dhcprelay.html
- http://support.microsoft.com/kb/837355/en-us
- http://207.46.16.252/en-us/magazine/2007.11.isavpn.aspx

8.1.2 Pour créer des connexions VPN site à site :

Pour plus d'informations, voir :
- http://www.labo-microsoft.com/whitepapers/20588/
- http://www.isaserver.org/tutorials/Implementing-IPSEC-Site-to-Site-VPN-between-ISA-Server-2006-Beta-Cisco-PIX-501.html