Installation d'un proxy web sous ISA server 2006

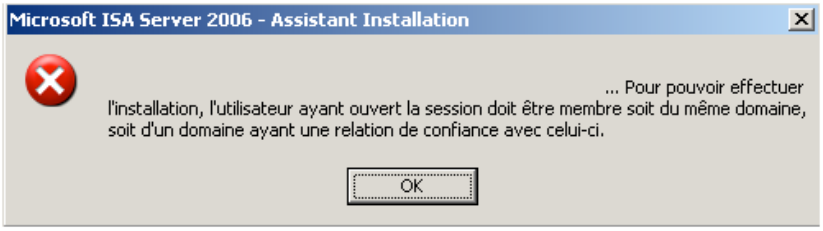
ISA Server est une passerelle de sécurité qui intègre un proxy (anciennement Proxy Server), un firewall et une gestion des VPN.

Plus d'info sont disponible sur : http://www.laboratoire-microsoft.org/articles/server/isa-server-2006/

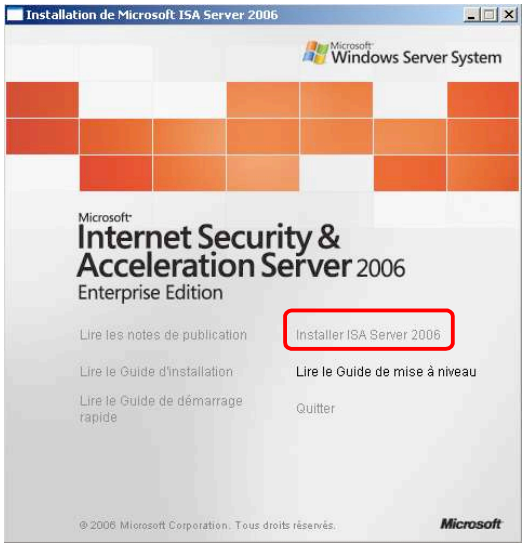
Installation

Isa Serveur sera installé sur un Windows 2003 server entreprise édition R2 32bit.

Connectez-vous sur le server avec un compte faisant partie du domaine.



Insérez l'ISO d'Isa server 2006 Enterprise Edition et cliquez sur « Installer ISA server 2006 ».



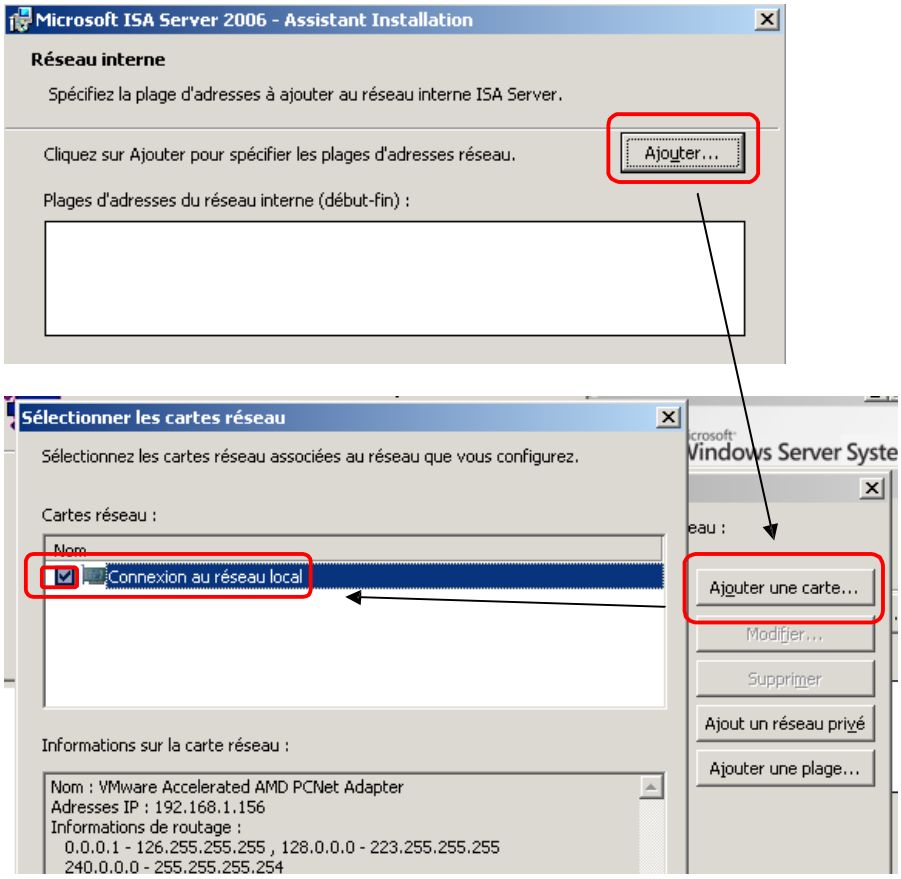
Cliquer sur « Suivant », acceptez les termes du contrat de licence puis renseignez le numéro de série.

Choisissez d' »Installer les services ISA server et un serveur de stockage de configurations ».

Dans notre cas le serveur contiendra la base de données (MSDE) de configuration, les logs… mais aussi les services, firewall et proxy d'ISA.

Laissez les composants par défaut.

Choisissez de créer un nouvel ISA server Enterprise, cliquez sur suivant lors de l'avertissement pour la création de nouvelle entreprise.



Dans notre cas plusieurs plages d'adresse (192.168.1.x, 192.168.2.x, 192.168.3.x, 192.168.4.x, 192.168.5.x et 192.168.12.x) doivent se connecter au proxy afin de ne pas saisir x plages nous ajouterons la carte réseau.

Autorisez la connexion des clients de pare-feu non cryptés malgré qu'ils ne soient pas pris en compte avec une configuration de proxy web.

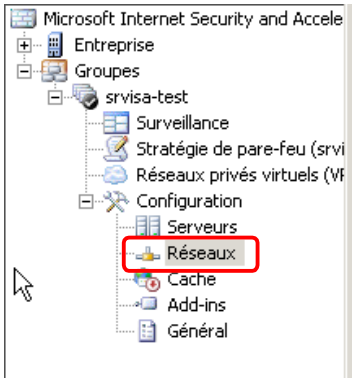
Le CD 2 de Windows 2003 server vous sera demandé pendant l'installation.

Cochez la case « Lancer la gestion d'ISA server après la fermeture de l'assistant » puis cliquez sur terminer.

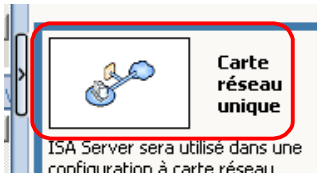
Configuration du modèle de sécurité

Cliquez sur le bandeau en haut pour accepter ou non de participer à l'amélioration du produit.

Développez l'arborescence jusqu'à la branche Réseaux



Puis choisissez le modèle de carte réseau unique



Cliquez alors sur suivant 2 fois puis validez le plan d'adressage proposé.

Validez l'application de la configuration de web proxy et de mettre en cache.

Sélectionnez Terminé.

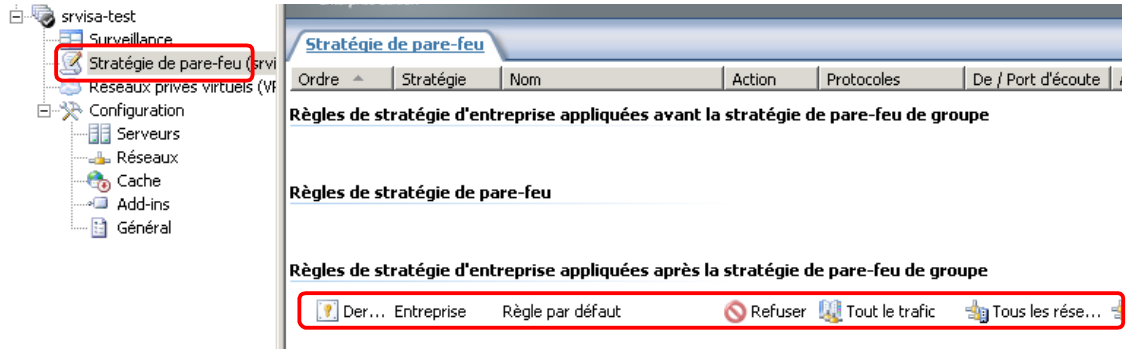
Pour information :

Pour plus d'info : http://www.isaserver.org/tutorials/ISA-Server-2006-Installing-ISA-2006-Enterprise-Edition-beta-Unihomed-Workgroup-Configuration.html

Configuration du proxy

A ce moment la les connexions sont bien filtrés, cependant rien ne passe :

Car le firewall est paramétré pour refuser tout le trafic.



Nous allons donc créer une règle de stratégie de pare-feu groupe autorisant tout le trafic à destination d'internet, notre but est dans un premier temps d'établir des logs et non de filtrer.

Cliquez alors sur Créer une règle d'accès :

Cliquez sur suivant puis « Autoriser les actions lorsque les conditions de la règle sont satisfaites », choisissez alors d' »appliquer la règle à tout le trafic sortant à l'exception de celui sélectionné » cela nous permettra par la suite de bloquer des applications, protocoles… (Attention vous devez au moins ajouter un filtre, vous pouvez sélectionner MSNM par ex).

Spécifiez alors que cette règle s'applique au trafic provenant du réseau interne et a destination de tout le réseau.

Spécifiez que cette règle s'applique à tous les utilisateurs, de cette manière les connexions « anonyme » mise à jour, skype… pourront se faire.

Il est possible de créer des groupes d'utilisateurs correspondant à utilisateurs membre d'une domaine LDAP.

Des règles pourront donc être associées à un groupe et non à un autre.

Pour cela cliquer sur l'onglet « Utilisateurs » puis sur le bouton « Ajouter », sélectionner alors un groupe (ISA) ou créer s'en un puis ajouter dans celui-ci des membres d'un domaine LDAP.

Il est aussi possible d'appliquer une règle sur une plage horaire définis, pour cela rendez vous sur l'onglet planification puis choisissez ou créez une planification. Activez alors celle-ci puis renseignez-la.

Validez cette règle.

Il nous reste alors à activer le cache d'ISA :

La taille maximal d'un fichier cache est de 64Go, il est possible de fractionner un fichier cache sur plusieurs lecteurs afin de le rendre supérieure à 64Go
La partition utilisée doit être formaté en NTFS, le lecteur doit être local.
Le lecteur devra être formaté et il est recommandé pour des raisons de performance d'accès disque de placer le cache sur un disque physique distinct du disque système.
Les « objets WEB »sont supprimés du cache si il n'y a plus de palce, il est donc intéressant de disposer d'un cache important afin de réduire les accès web
L'analyseur de performance de l'OS gère les performances du cache d'ISA

Faîtes alors un clic droit sur le serveur ISA puis cliquez sur Propriétés ?

Renseignez alors l'emplacement du cache ainsi que sa taille.

Une fois cela fait, la navigation WEB par le cache et avec des log sera activé.

Rapport

Il est intéressant de créer un log hebdomadaire du trafic WEB.

Pour cela allez dans surveillance puis dans l'onglet rapport et cliquez sur « créer et configurer les tâches de rapport ».

Cliquez alors sur Ajouter puis renseignez un nom de tâche, sélectionner alors le contenu à inclure dans le rapport. Choisissez la fréquence des envoies.

Créez alors un emplacement auquel les personnes qui recevront ce rapport pourront avoir accès en lecture et spécifiez cette emplacement dans la zone « Dossier des rapports publiés » vous pouvez aussi spécifier un compte dédié à l'écriture du rapport.

Renseigner alors les valeurs permettant la notification par mail, cochez la case « Inclure un lien vers le rapport final dans le message » puis cliquer sur terminer.

N'oubliez pas d'appliquer ces changements.

Visualisation des rapports créés automatiquement.

Isa server va créer automatiquement des journaux, il est possible de paramétrer ceux-ci.

Pour cela rendez vous dans « Surveillance » puis dans l'onglet « Journaux ». Dans la partie de droite cliquer sur « Configurer les journaux du proxy WEB ».

Dans notre cas le stockage est effectué par une Base de données MSDE, dans les options il est possible de définir le chemin de stockage des logs (chemin par défaut) et surtout la taille limite des logs (800Go) et l'espace libre à préserver sur le disque (8Go). Vous pouvez ici définir la suppression des données de plus de x jours (700jours).

Le logiciel MDF Viewer permet de visualiser les logs historié, les logs de la journée ne sont pas disponibles.

Disponible : http://www.redline-software.com/fra/products/tk/components/mdf_viewer.php

Cependant SQL Server Management Studio permet de visualiser les logs de la journée mais aussi ceux historiés.

Une installation de SQL Server Management Studio par défaut permettra de visualiser l'ensemble des logs y compris sont ceux de la journée.

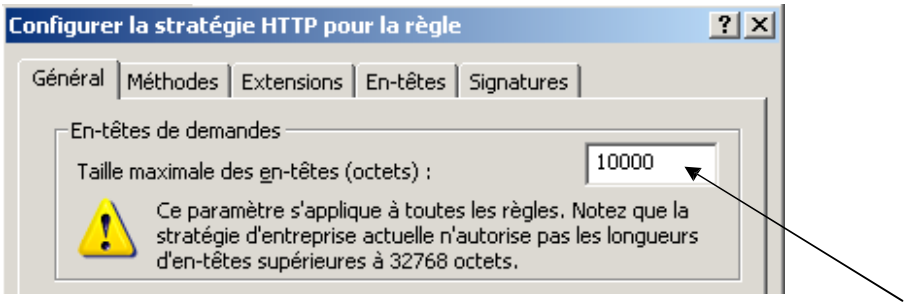
ISA server crée une base de données par jours.

Il existe une application Java crée par Mathieu Passenaud qui effectue des requêtes SQL nécessaire à l'élaboration d'un rapport sur l'utilisation du WEB par utilisateurs… (Demande de la direction).

Filtrage du proxy

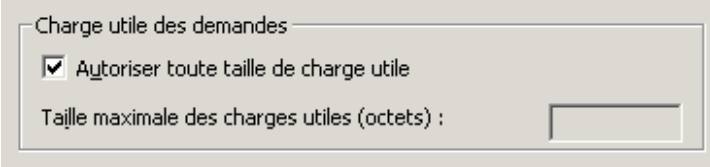
ISA server permet d'effectuer différents niveau de filtrage WEB, pour y accéder il faut faire un clic droit sur la règle de pare-feu groupe précédemment créée puis sélectionner configurer http dans le menu contextuel.

Cette fenêtre va nous permettre de configurer différente action.



Afin de réduire les attaque WEB Isa serveur préconise de limiter la taille des en-têtes de demande à 10Ko et de l'augmenter si besoin est ? (Type d'attaques par dépassement de tampon, attaques par déni de service…)

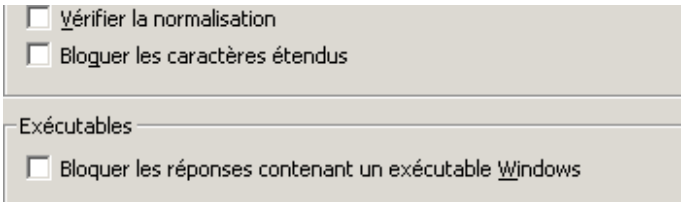
Il est possible de spécifier la taille max de donnée pouvant être envoyées/publiées par un utilisateur par la zone « Charge utile des demandes :



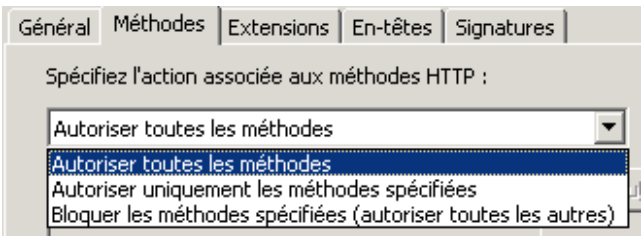
ISAS recommande d'imposer une taille max de 10Ko au requête d'URL (syntaxe placé après le ? de l'URL).

> (Les requêtes longues et les URL sont des vecteurs d'attaque connus pour les vers circulant sur Internet. Ces vers transmettent une demande GET longue et utilisent l'URL pour incorporer leur charge utile.)

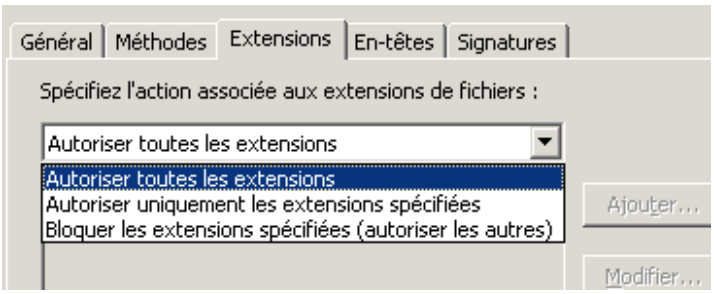
Il est possible de demander de vérifier la normalisation, de bloquer les caractères étendus et de bloquer les réponses contenant un exécutable Windows.



Il est possible d'effectuer des actions sur les méthodes http (GET, POST, HEAD…)



ISAS permet de bloquer des extensions .EXE, .BAT …



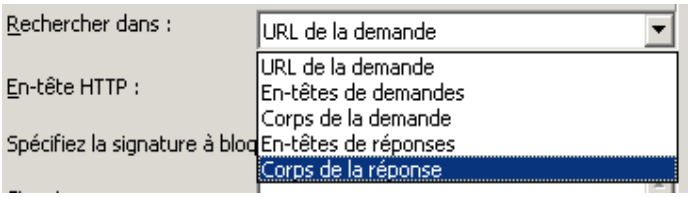
ISAS gère aussi les en-têtes de demande et de réponse HTML (entre balise <head> et </head>)

Il permet de les bloquer, de les modifier ou de les renvoyer sous une autre forme.

Il est aussi possible de gérer les signatures sur les URL de demande, sur les en-têtes de demandes/réponses ou sur le corps de réponses ou de demandes.

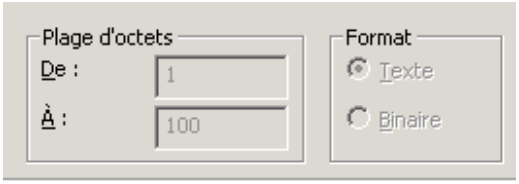
Les signatures correspondent à des caractères, mot clés, expression…

Pour cela renseigner la zone de critère de recherche :



Puis renseigner la signature qui correspond au caractère, mot clé, expression…

Cliquer sur Ok, attention par défaut la plage d'octets filtrées est de 100octect.



Exemple de signature : http://technet.microsoft.com/fr-fr/library/cc302520(en-us).aspx

Il est possible à l'aide du moniteur réseau intégré à Windows 2003 Server de trouver des signatures à l'aide d'une machine cliente.

En effectuant un clic droit sur la règle de pare-feu groupe précédemment créée il est possible d'activer les téléchargements FTP (ceci est désactivé par défaut), il est aussi possible de désactiver les protocoles RPC supplémentaire tel que DCOM