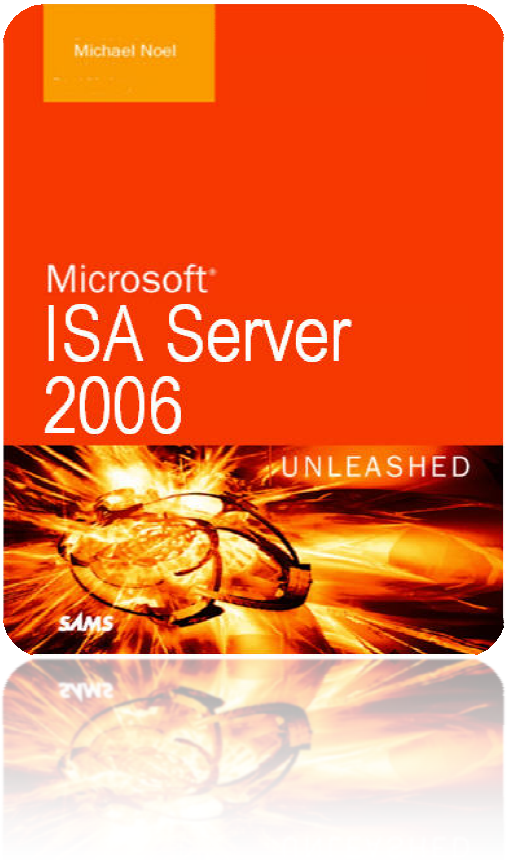
TAGREROUT
Seyf Allah
TMRIM



Projet Isa server 2006

Installation et configuration d'Isa server 2006 :

- **Installation d'Isa server 2006**
- **Activation des Pings**
- **NAT**
- **Redirection DNS**
- **Proxy (cache, visualisation des journaux)**

Table des matières

Qu'est-ce qu'ISA Server ?

ISA Server 2006 est la passerelle de haute sécurité qui protège votre informatique contre les menaces en provenance d'Internet, tout en offrant à vos utilisateurs un accès à distance rapide et sécurisé aux données et aux applications

Présentation d'ISA Server :

Face à l'explosion de croissance des activités basées sur Internet et au nombre considérable de réseaux d'entreprise qui y sont connectés, il est plus que jamais nécessaire de disposer d'une passerelle puissante et facile à administrer qui fournisse une connexion sécurisée tout en augmentant et améliorant les performances réseau. ISA Server répond à ces exigences par une solution de connectivité Internet contenant à la fois un pare-feu d'entreprise et une solution de cache Web complète. Ces services sont complémentaires : vous pouvez utiliser l'une ou l'autre de ces fonctionnalités, ou les deux, lorsque vous installez ISA Server sur votre réseau.

ISA Server protège votre réseau, vous permettant de mettre en œuvre votre stratégie de sécurité d'entreprise en configurant un large ensemble de règles spécifiant quels sont les sites, les protocoles et les contenus qui peuvent transiter par ISA Server. ISA Server surveille les échanges de demandes et de réponses entre Internet et les ordinateurs clients internes, contrôlant qui est habilité à accéder aux ordinateurs du réseau de l'entreprise, et auxquels. ISA Server contrôle également quels sont les ordinateurs, sur Internet, auxquels les clients internes peuvent accéder.

ISA Server propose de nombreuses options de sécurité, notamment la détection d'intrusion et de filtrage de paquets. Vous pouvez créer des stratégies d'accès basées sur des informations au niveau de l'utilisateur ou des adresses IP (Internet Protocol) et déterminer les cas dans lesquels la règle doit être appliquée.

ISA Server permet la publication sécurisée. Il permet de définir une stratégie de publication qui protège les serveurs de publication internes et autorise les clients Internet à y accéder en toute sécurité.

ISA Server implémente un cache contenant les objets souvent demandés. Vous pouvez configurer le cache pour vous assurer qu'il contient les données les plus fréquemment utilisées par l'organisation ou les plus souvent sollicitées par vos clients Internet. Le cache d'ISA Server peut être distribué sur de nombreux serveurs ISA par groupes ou chaînes de groupes. Ceci peut permettre de réaliser des économies sur le coût des connexions Internet, car les clients peuvent obtenir les données provenant du cache d'ISA Server le plus proche.

ISA Server est extensible. L'Utilitaire de gestion ISA possède une interface COM correspondante que les administrateurs peuvent programmer à l'aide de langages de programmation de haut niveau ou de langages de création de scripts. La principale fonction de pare-feu peut être étendue par d'autres développeurs implémentant des filtres Web ou d'application. La fonctionnalité de cache peut être améliorée à l'aide de l'interface de programmation d'application (API) du cache. L'interface de l'Utilitaire de gestion ISA peut être étendue afin de fournir des outils d'administration intégrés pour les nouvelles extensions.

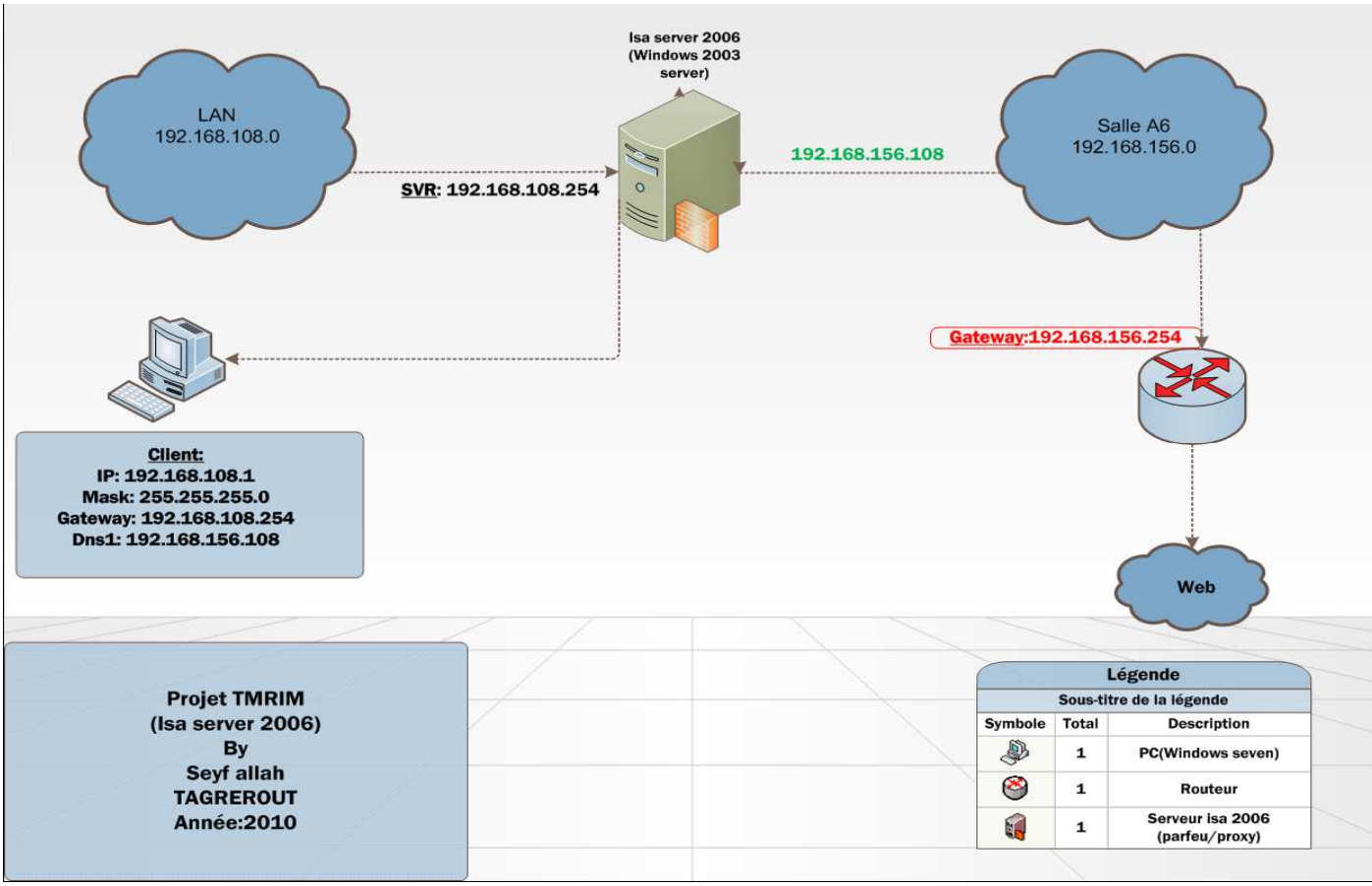
Présentation du projet :

Dans le cadre du projet en 2eme année de bac pro MRIM, on a eu la chance d'effectuer un projet sur **Isa server 2006**, dans le quel on a effectué plusieurs tâches**. Ce projet est fait en binôme mais n'ayant pas de partenaire j'ai du amené a bout ce projet tout seul.**

Voici les taches que j'ai effectuées durant ce projet :

- **d'activation des Pings**
- **Accès internet par NAT**
- **Publication du service DNS**
- **Proxy**

Voici le schéma du travail que j'ai effectué sur Isa server 2006 :

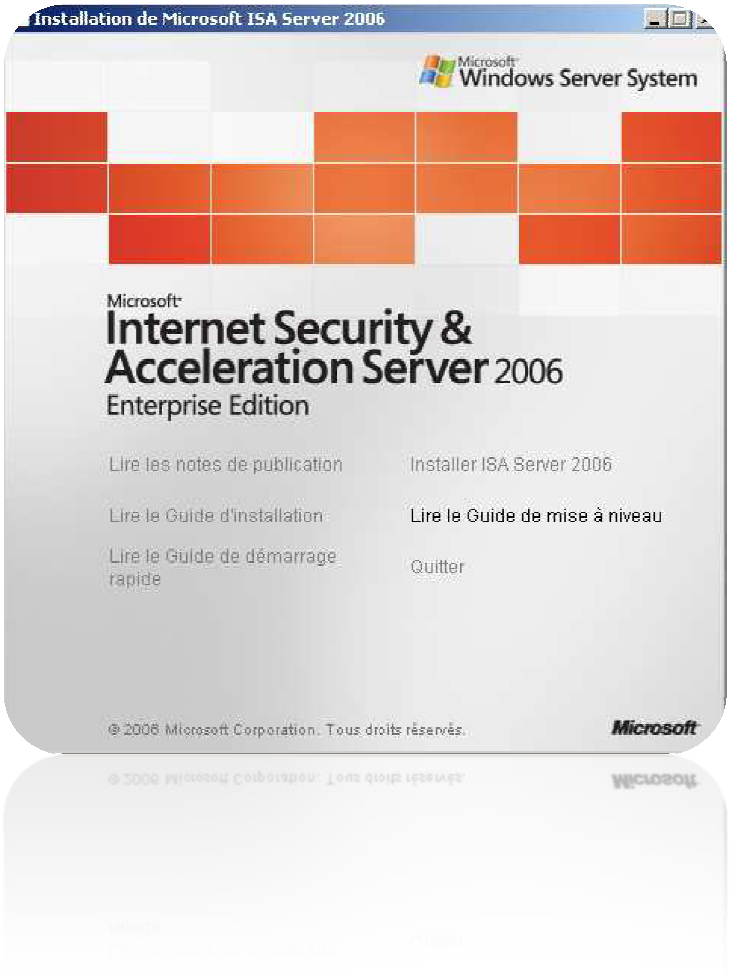


Procédure d'installation d'Isa Server 2006 :

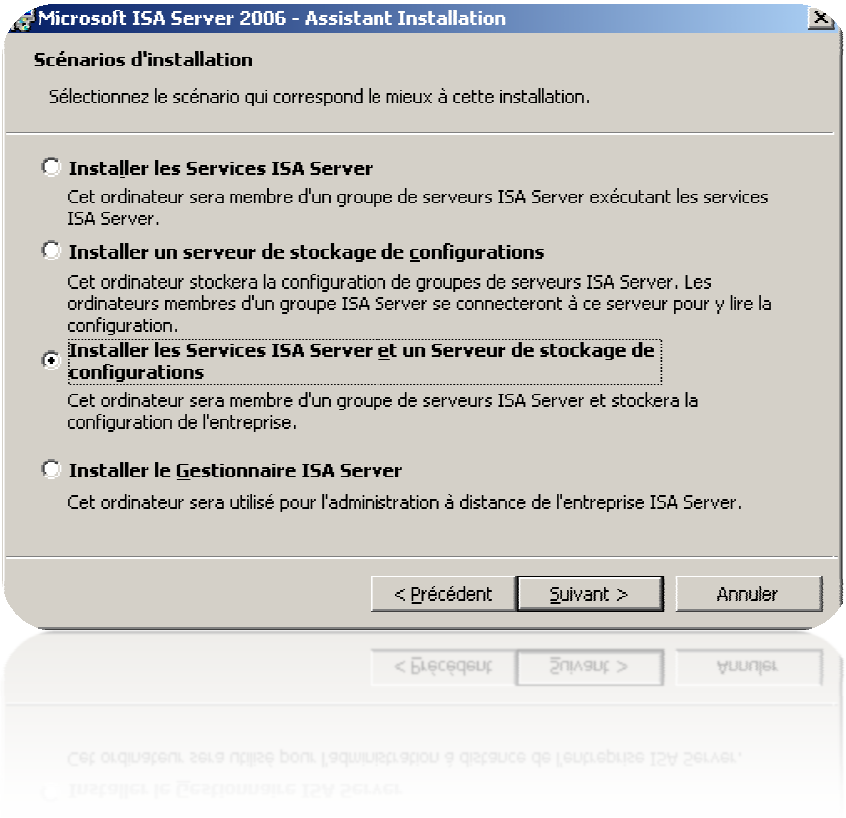
Bien sur pour effecteur cela, il a fallu installer et configurer Isa server 2006.
D'après mon sommaire je vais dés à présent vous présenter l'installation d'Isa server
Faut savoir qu'Isa server peut s'installer que sur des systèmes d'exploitation pour serveur (Windows server 2000,2003 ou 2008).Avant d'installer Isa server 2006 faut au préalable installer sur Windows 2003 le service pack 1 sinon l'installation d'Isa server sera impossible.

Après avoir installé **le service pack 1** sur le serveur (Windows serveur 2003), on peut commencer l'installation d'Isa server 2006 sur notre serveur.

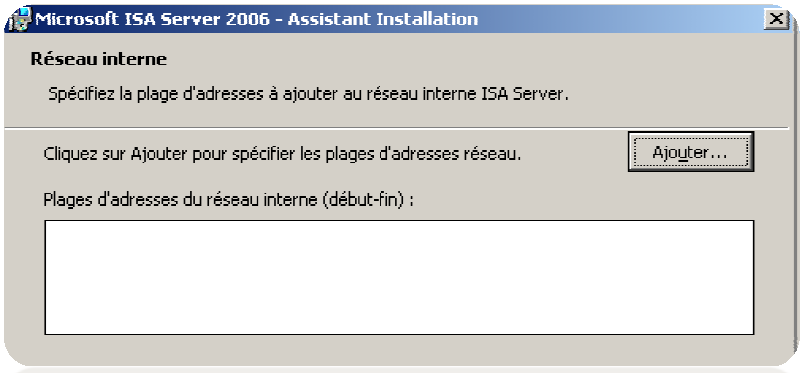
1) : Insérez l'ISO d'Isa server 2006 Enterprise Edition et cliquez sur « Installer ISA server 2006 ».



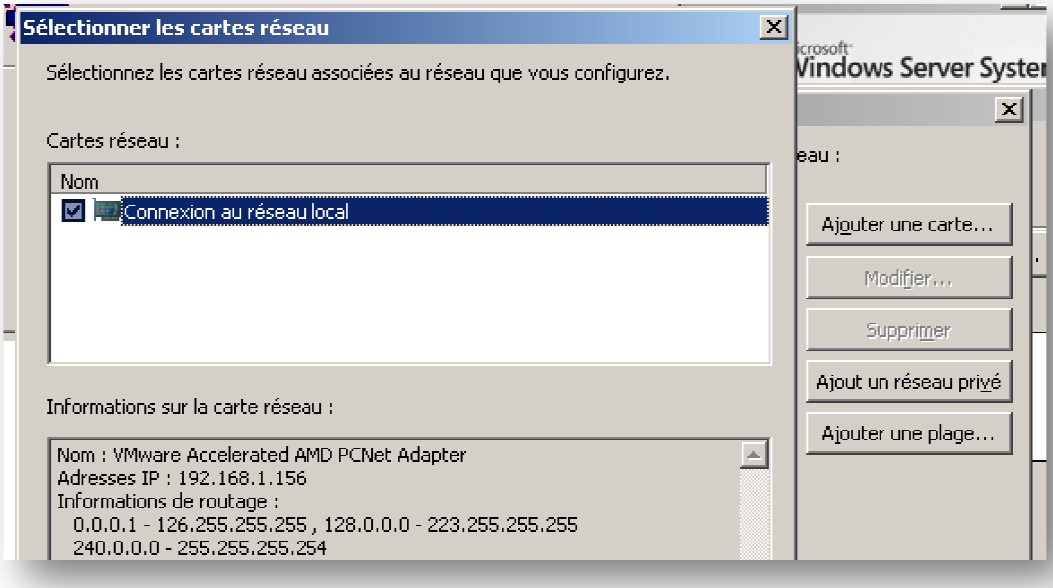
2) : Cliquer sur « Suivant », acceptez les termes du contrat de licence puis renseignez le numéro de série



3) : 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.



On clique sur ajouter, La suite est à la page suivante.



4) :

Dans notre cas plusieurs plages d'adresse (192.168.108.0 jusqu'à 192.168.108.255)
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.

Après cette opération l'installation d'Isa server 2006 débute et se termine au bout de 20minutes à peu prés.

Voici à quoi ressemble Isa server 2006 :

Procédure d'activation des Pings :

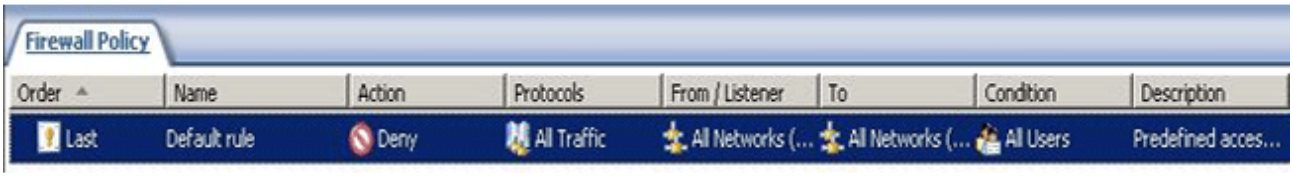
Après l'installation d'Isa server je vais vous présenter la procédure d'activation de pings à partir de mon client sur mon serveur (SVR8)

Activer le Ping pour ISA Server, mais pas d'une source ouverte réseau, il suffit de permettre à partir d'une liste de machines, à partir des ordinateurs de gestion à distance

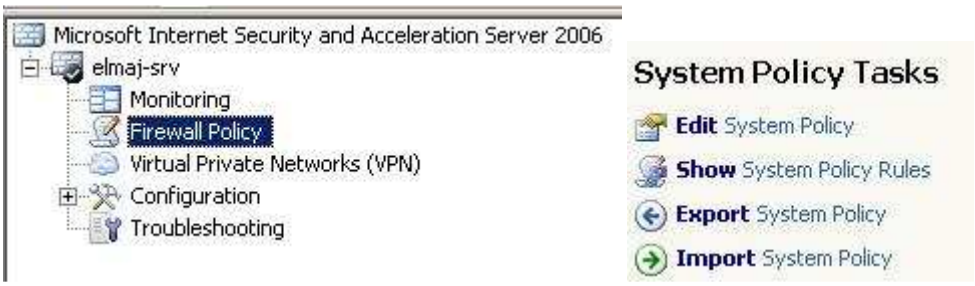
Configuration :

1) : Ouvrez ISA Server Management Console, cliquez sur **Démarrer> Tous les Programmes**> **Microsoft ISA Server**> **Gestion ISA Server.**

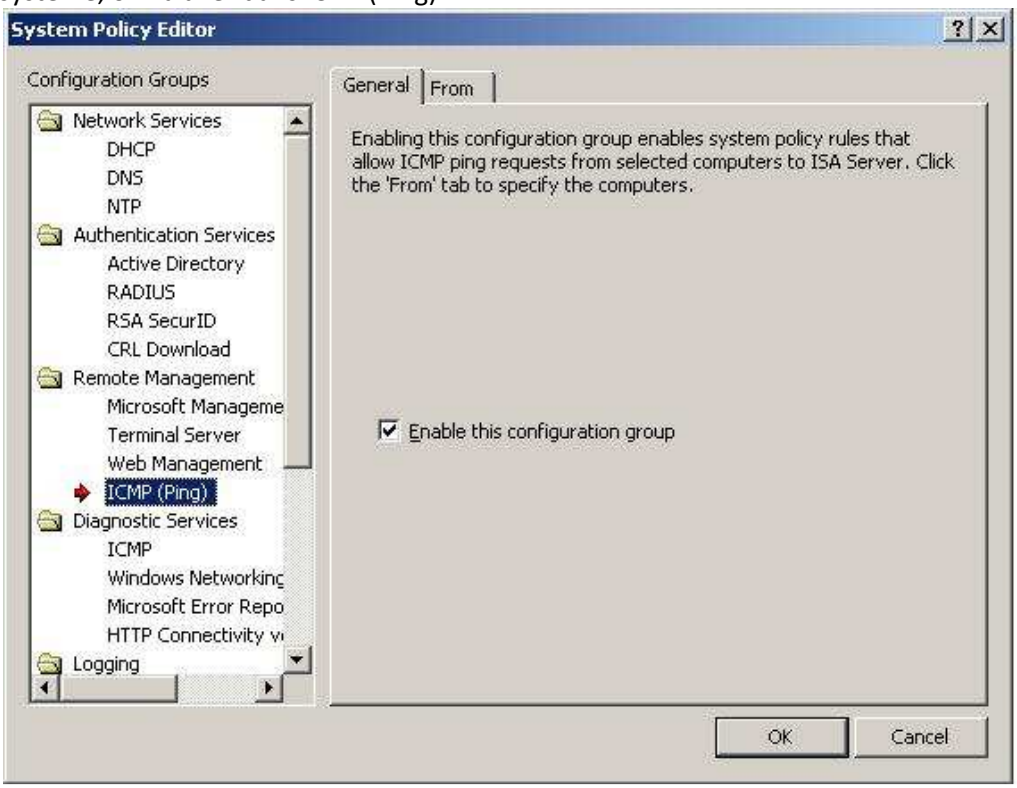
2) : Cliquez sur le **nœud** Stratégie **de pare-feu,** comme vous pouvez le voir, il s'agit d'une nouvelle installation de ISA Server 2006, et elle a encore sa valeur par **défaut règle de refus.** Nous ne créerons pas une nouvelle règle afin de permettre Ping pour ISA Server, nous allons travailler avec ISA Server System stratégie,



3) : Sur le panneau de droite, sous l'onglet **Tâches,** cliquez sur la **politique d'édition du système**



La fenêtre s'ouvre et nous allons dans notre cas ici dans travailler avec une seule règles de stratégie système, on va aller dans ICMP(Ping).

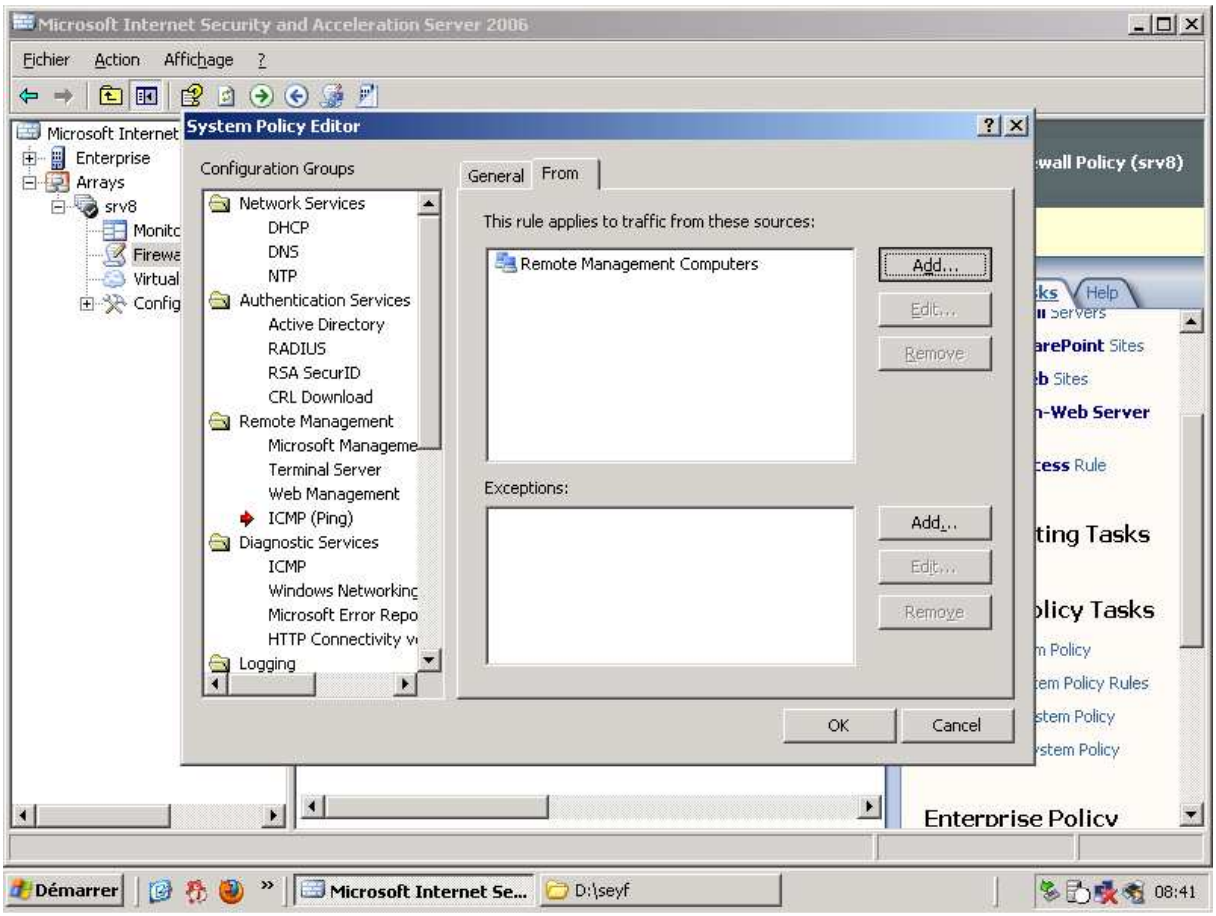


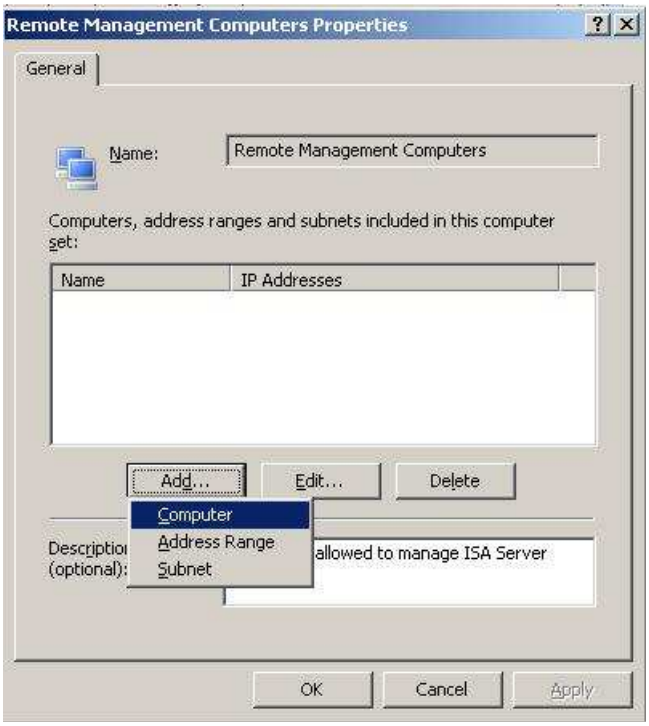
Par défaut, ICMP (Ping) est activé, alors pourquoi personne ne peut faire un Ping sur le serveur ? C'est parce que vous aurez besoin pour préciser de quelle machine (s) que vous allez autoriser le Ping à votre serveur ISA, cela peut se configurer en cliquant sur l'onglet À partir de, par défaut des ordinateurs de gestion à distance est inclus sous l'onglet À partir, et Par défaut. Les ordinateurs de gestion à distance sont vides et vous devrez le remplir. Parce que c'est vous aurez besoin de préciser quelle machine (s) que vous allez Autoriser le Ping à votre serveur ISA.

Cela Peut se Configurer en cliquant sur l'onglet À partir de, par défaut des ordinateurs de gestion à distance est inclus à Sous l'onglet À partir, et Par défaut, les ordinateurs de gestion à distance à vide Est et devrez vous le Remplir.

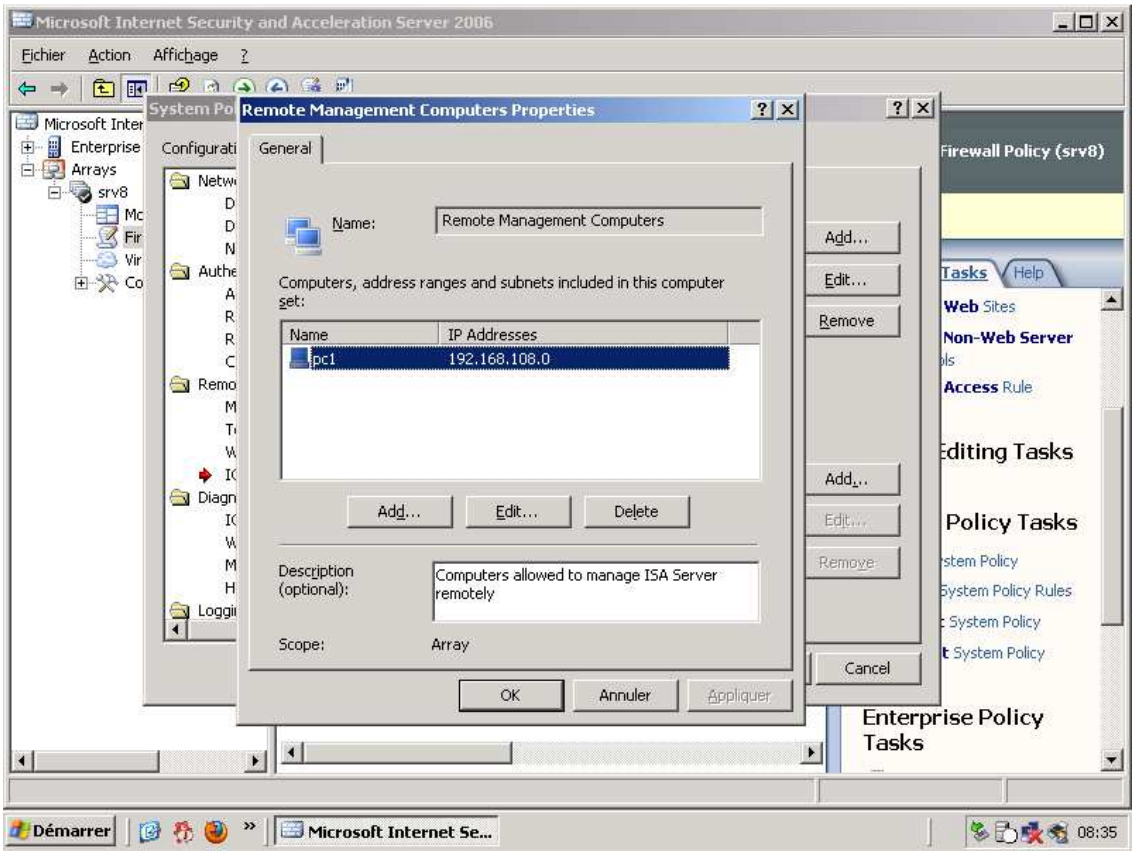
Je clique sur From pour ajoute la station qui va pouvoir effectuer un Ping sur mon serveur.

Je clique sur add



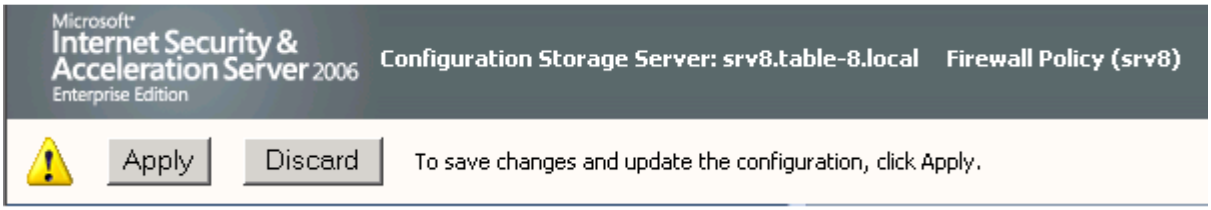


Je vais dans **ADD** pour ajouter une station.



On voit bien que j'ai ajouté ma station ici (PC1) avec le sous-réseau 192.168.108.0

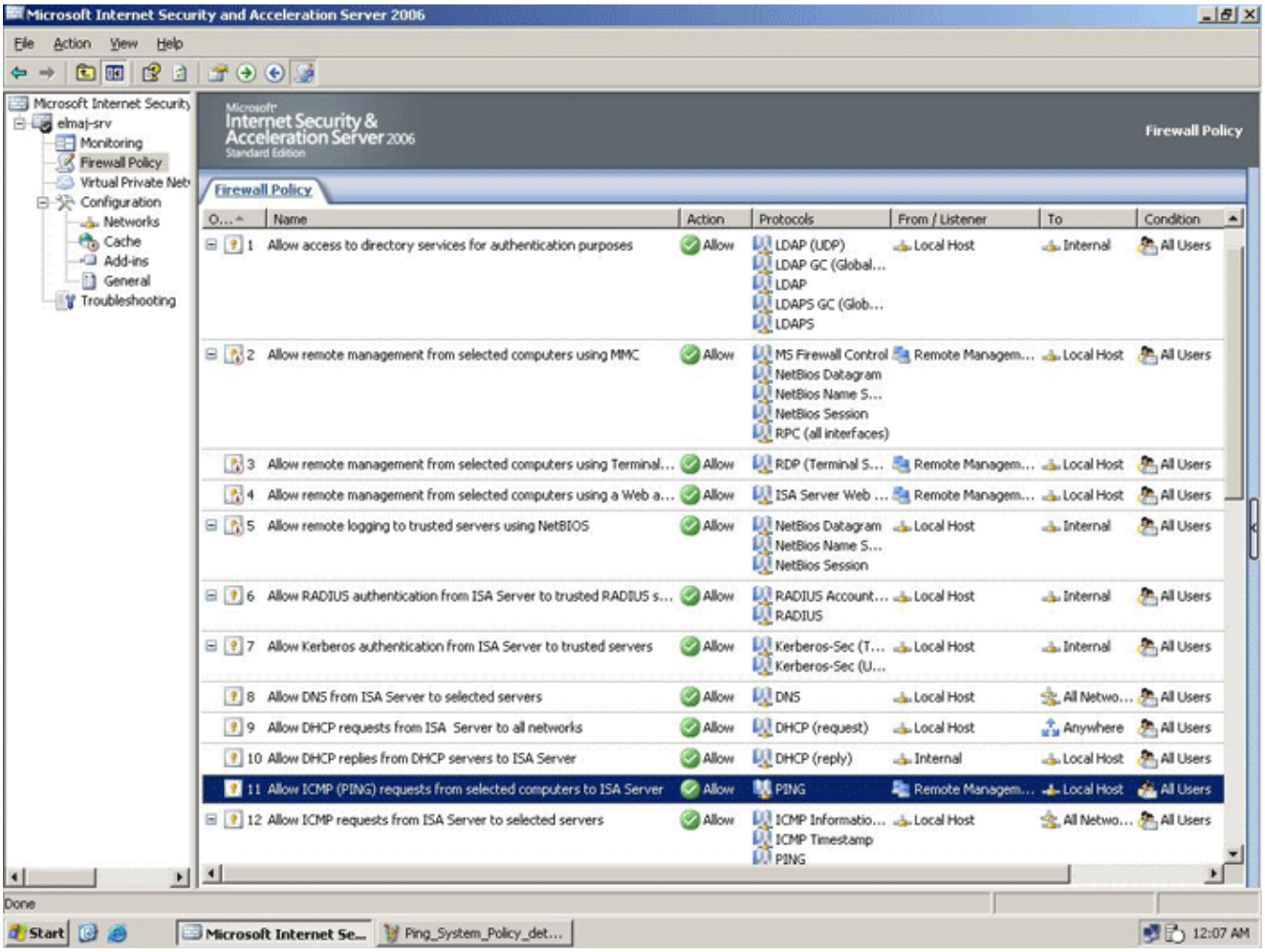
Après cette opération on fait appliquer pour que la configuration qu'on a effectuée soit prés en compte.



Je clique ici sur le icône entouré en rouge pour voir toutes les règles et notamment la règles d'activation de Ping que j'ai effectuée auparavant

La suite page suivante.

On peut voir ici que la règle pour activé le Ping est bien activé.

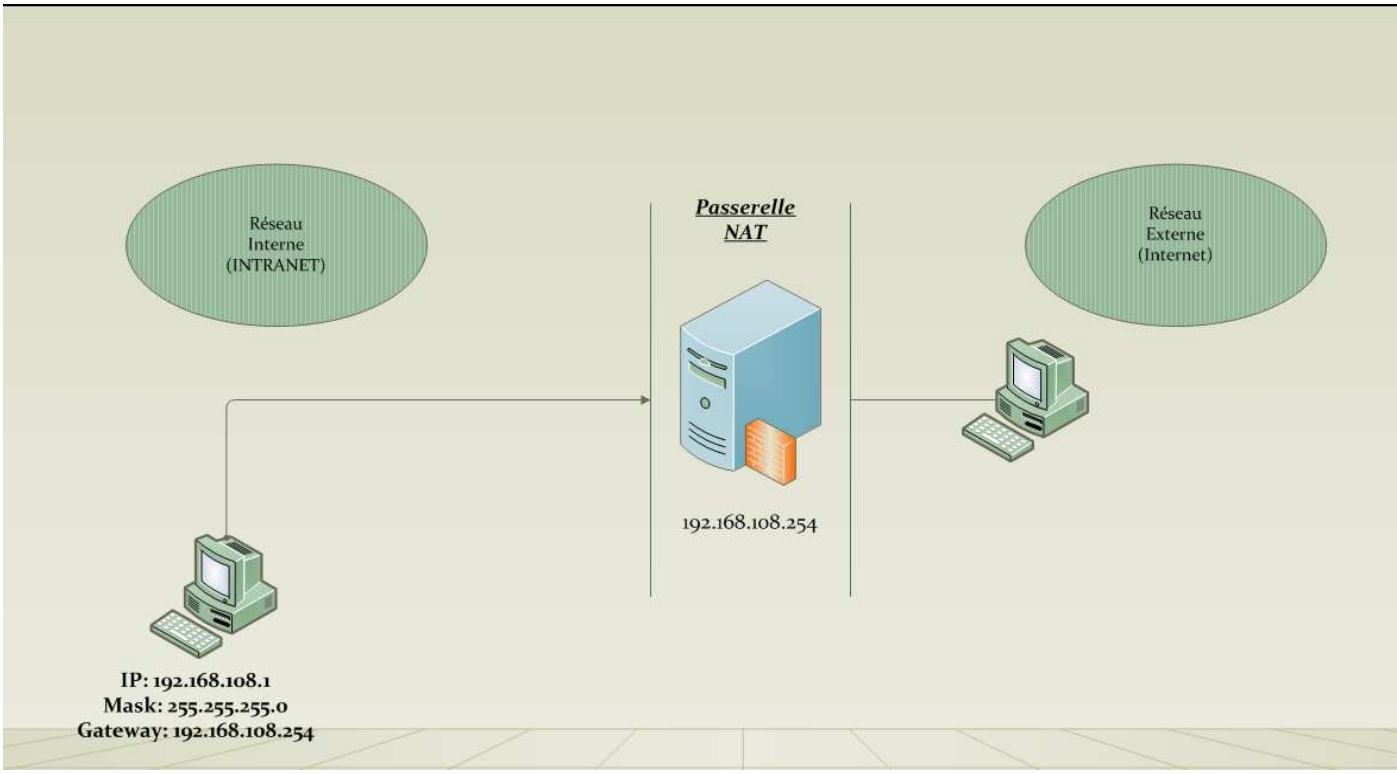


La première configuration terminé je vais vous montrez dés à présent la mise en ouvre un NAT avec ISA server 2006 La suite se déroule à page suivante.

Tout d'abord je vais vous présenter le NAT :

Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.

Voici un schéma du NAT dans mon projet :



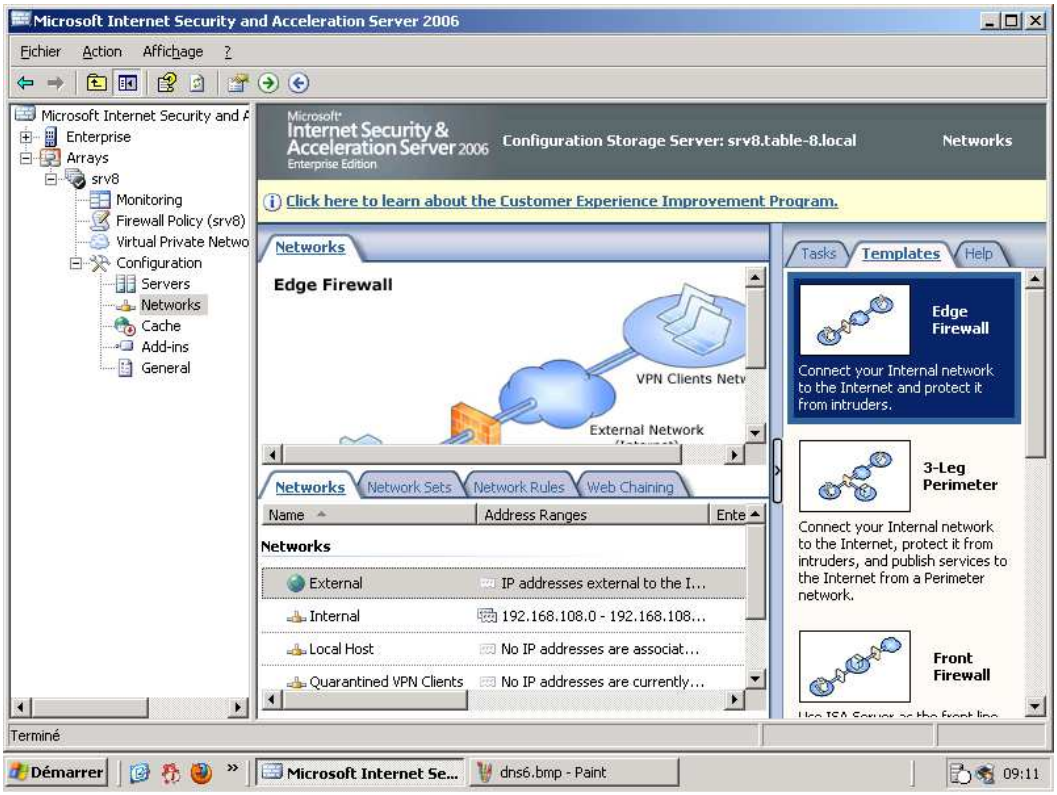
Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction ») des paquets provenant du réseau interne vers le réseau externe.

Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande.

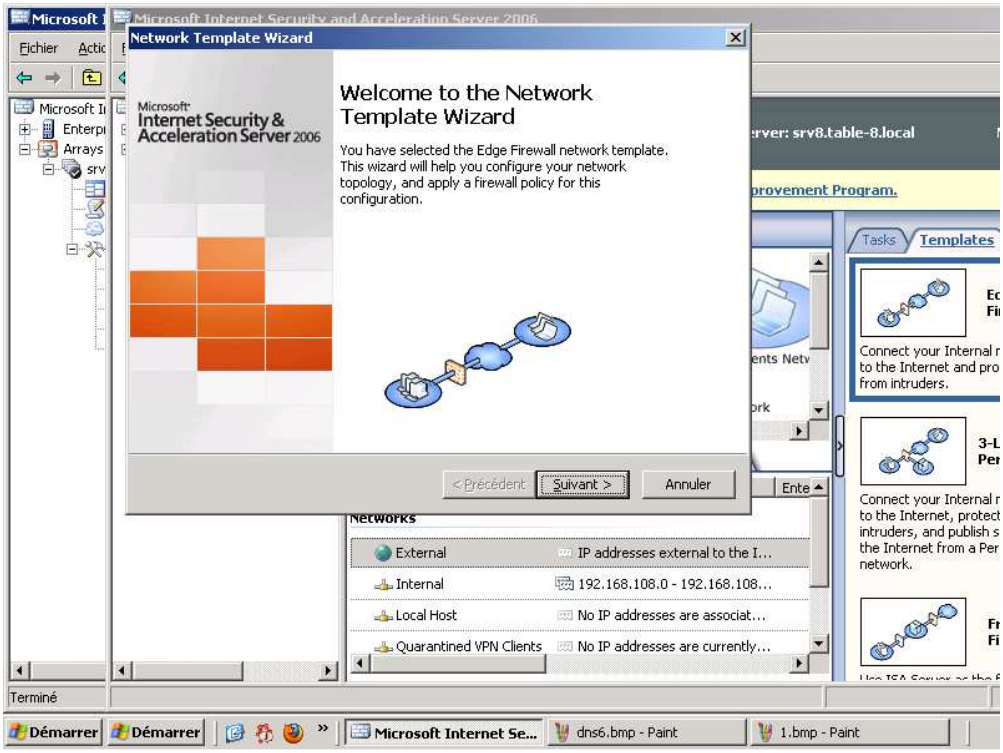
Pour configurer cela il suffit de faire la manipulation suivante :

Pour configurer cela il suffit de faire la manipulation suivante :

On va dans **(Networks)** et après on clique sur **(Templates)**
on va sur **EDGE FIREWALL.**

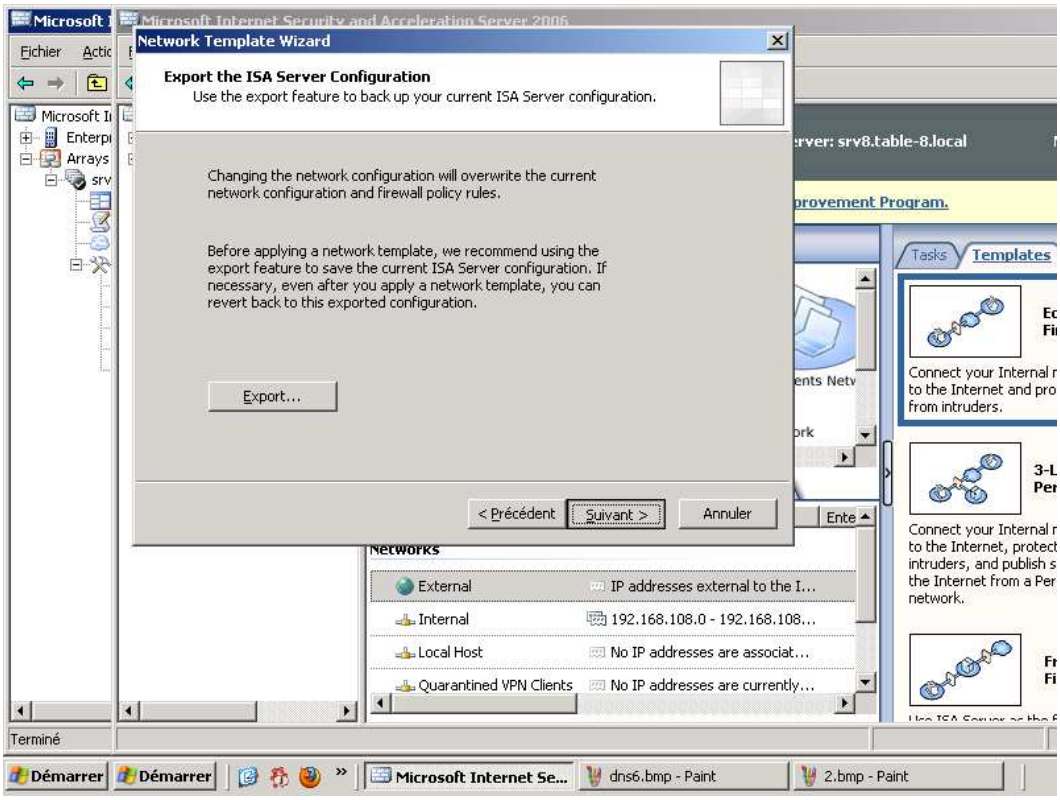


Après avoir choisi l'option **Edge Firewall** on va voir apparaitre cette fenêtre :

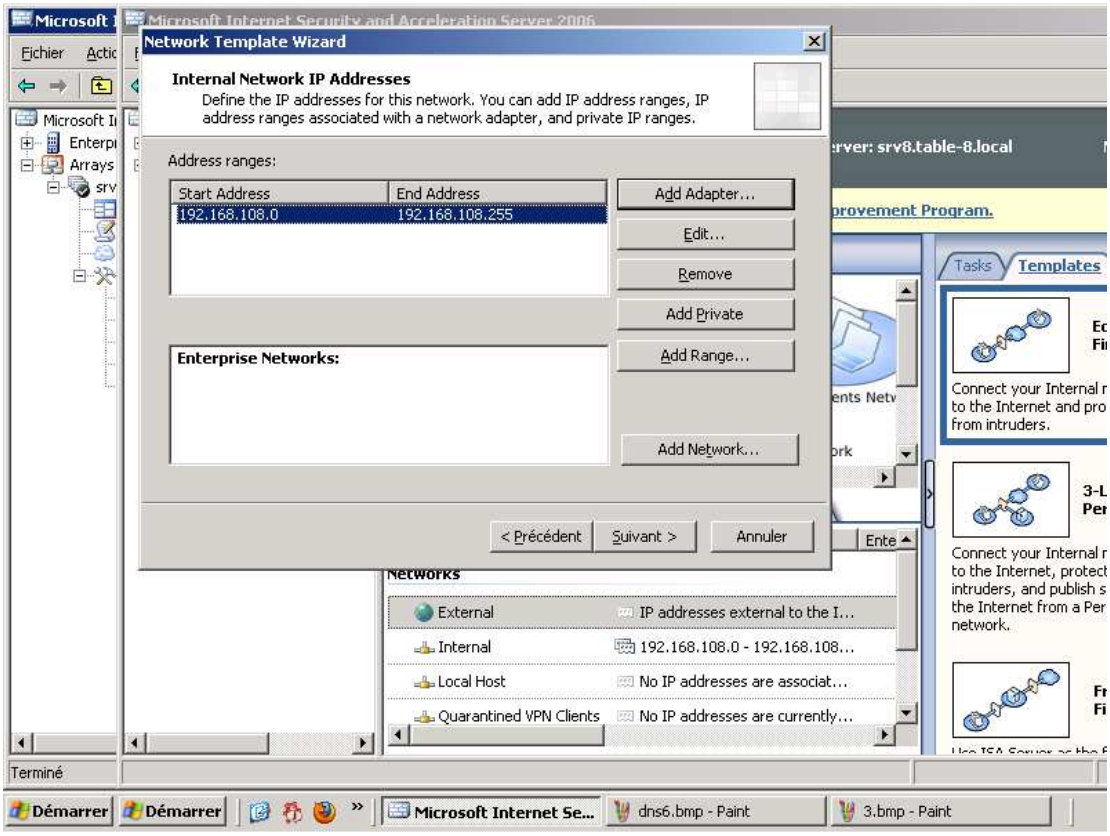


On clique sur suivant.

On clique encor sur suivant :

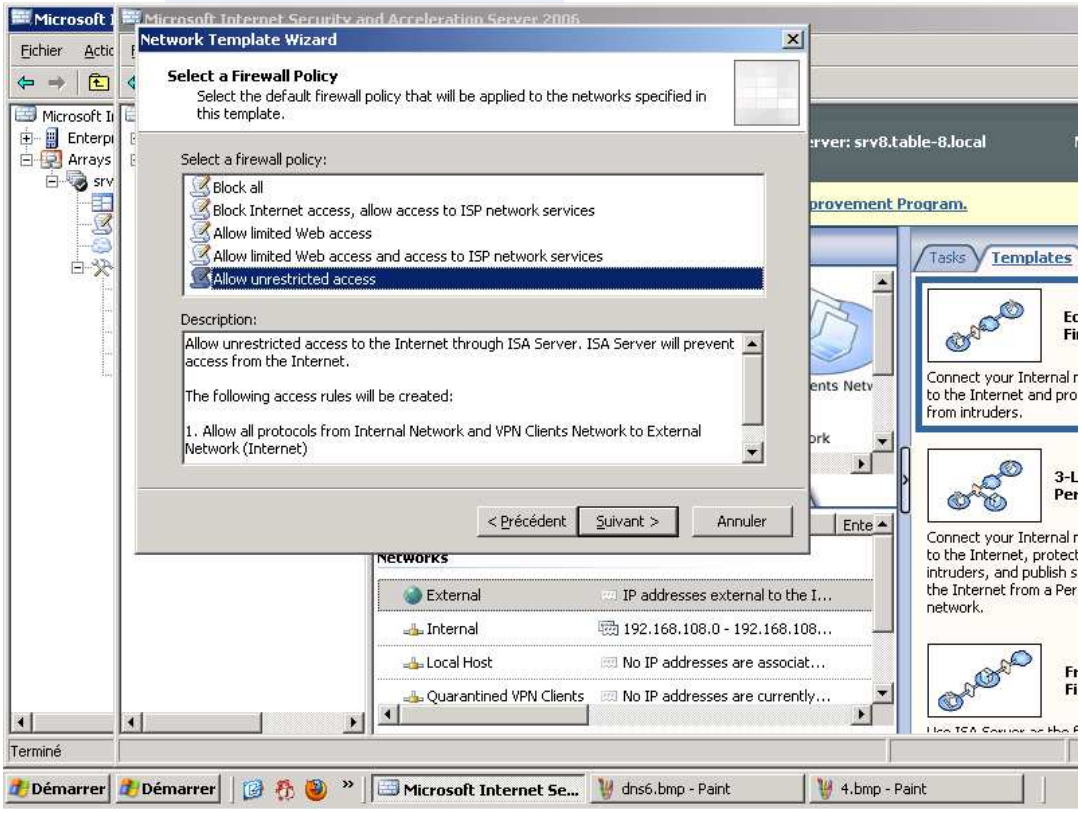


Et après dans (ADD Adapter) on rentre la plage de notre adresse IP (coté INTERNE)

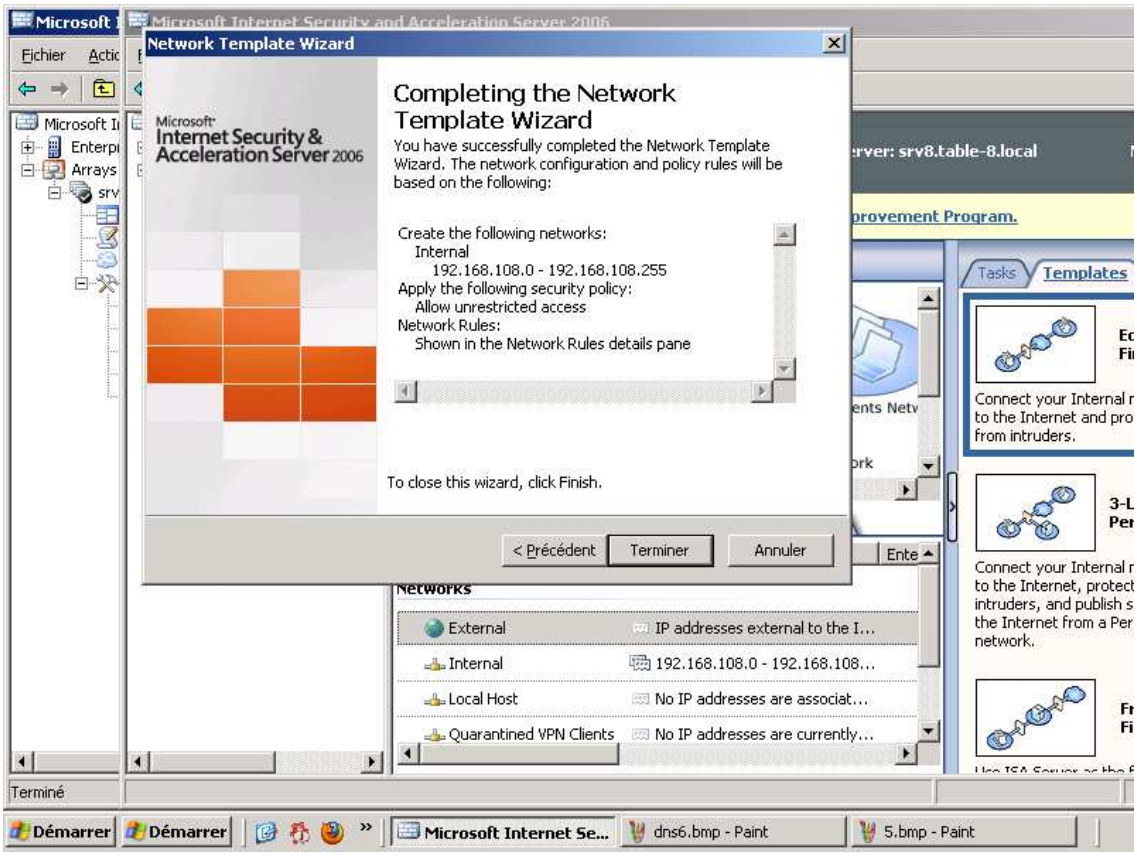


On clique sur suivant.

Ensuite on choisi l'option (allow unrestricted Access)
C'est à dire **(autoriser l'accès sans restriction)**

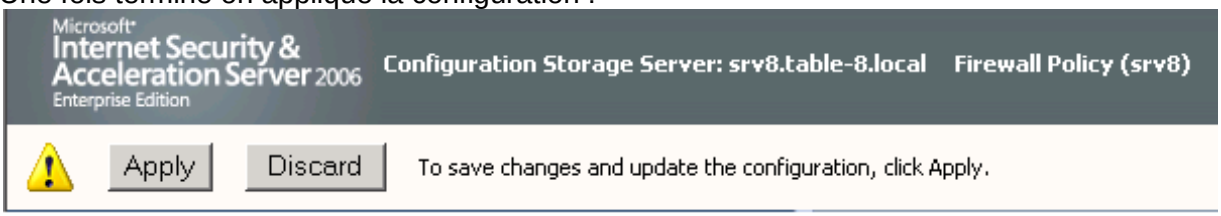


Ensuite :



On voit bien la plage de mon réseau (interne) donc pour finir
On clique sur terminé

Une fois terminé on applique la configuration :



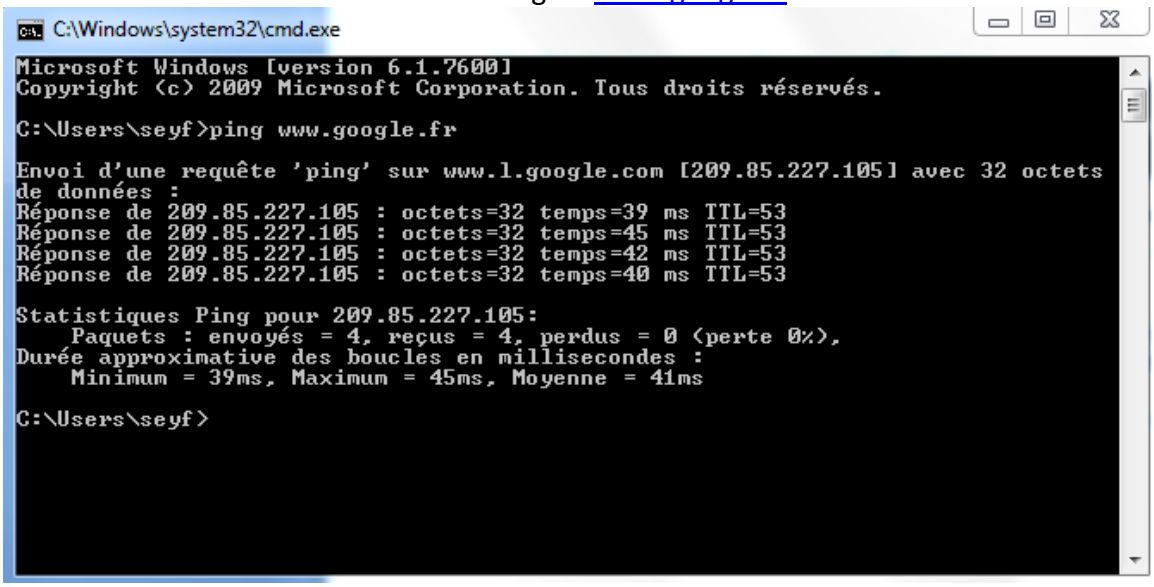
Pour vérifier que notre NAT fonctionne, on va sur un client qui est relier bien sur a la 2eme interface de Isa server 2006 coté (interne) et on va essayer d'aller sur le net et de faire un ping de www.google.fr
Avant de faire cela il faut rentrer la configuration IP suivante sur le client :

IP : 192.168.108.1
Mask : 255.255.255.0
Gateway: 192.168.108.254

Pour le DNS vu qu'on n'a pas encor effectué la publication DNS, je suis obligé de mettre le DNS du FAI

DNS : 86.64.145.146

Une fois ces paramètres entrés dans le client on va pourvoir tester notre NAT, en ouvrant une fenêtre MS-DOS et on fessant un Ping de www.google.fr comme ce ci :



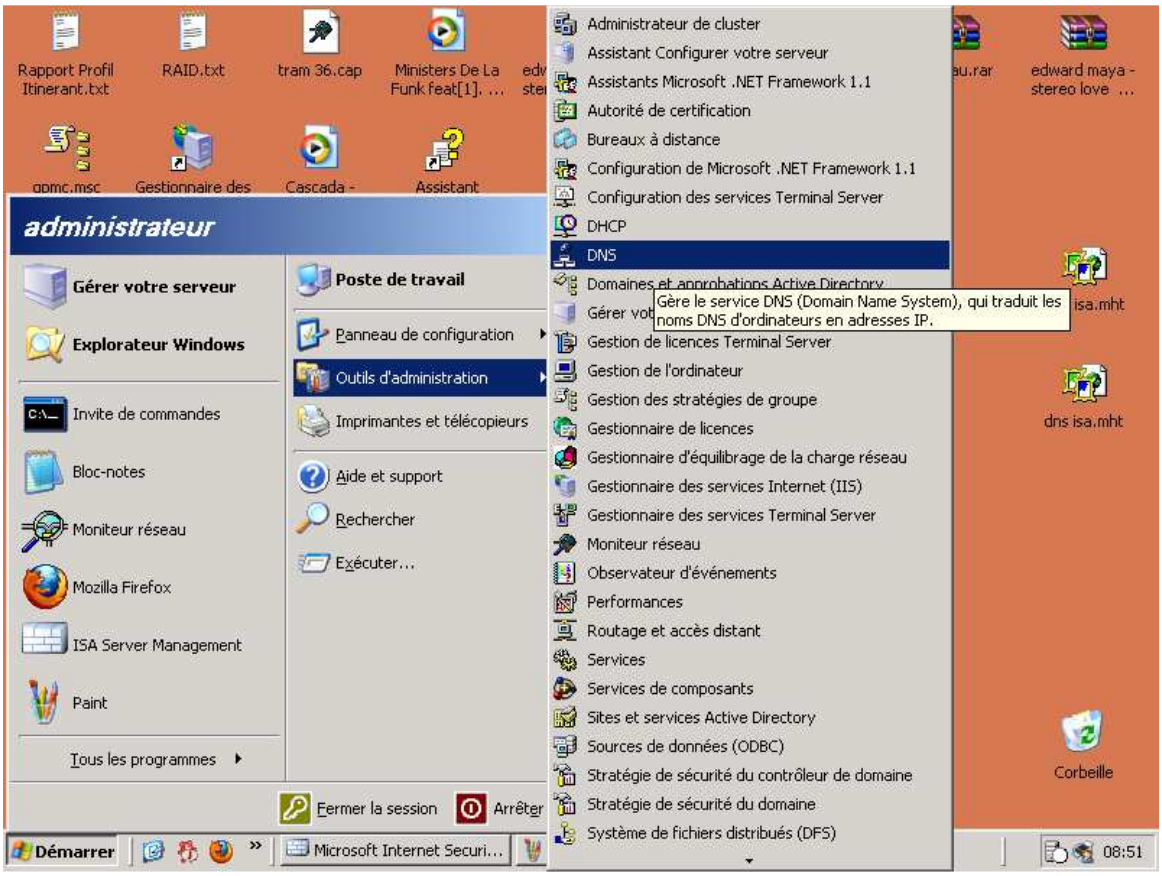
On voit bien qu'il ya une réponse du site de **Google.**
Conclusion : notre NAT fonctionne parfaitement

Pour le champ TTL :
La durée de vie : du paquet (*TTL*, *Time To Live*). Le champ de durée de vie (TTL) permet de connaître le nombre de routeurs traversés par le paquet lors de l'échange entre les deux machines. Chaque paquet IP possède un champ TTL positionné à une valeur relativement grande. A chaque passage d'un routeur, le champ est décrémenté. S'il arrive que le champ arrive à zéro, le routeur interprétera que le paquet tourne en boucle et le détruira.

Après avoir configurer le NAT, on va s'occuper de la publication DNS de manière a ce qu'on mettent notre serveur DNS qu'ici est (192.168.156.108)
Pour cela on va procéder de la façon suivante :

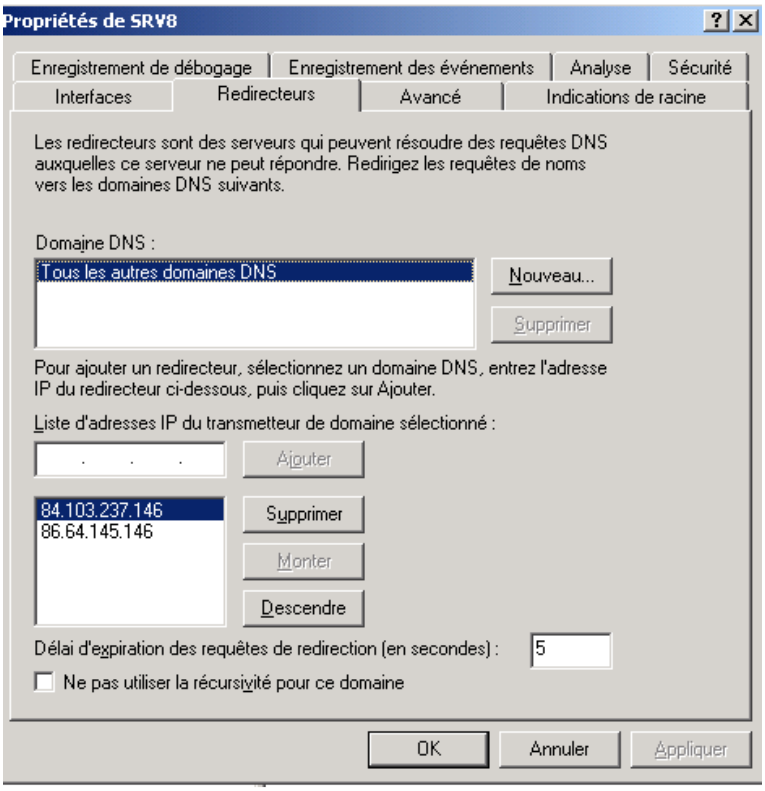
Je commence par la Configuration sur le serveur DNS :

1) : Cliquez sur **Démarrer** .pointez sur **Outils d'administration**, puis cliquez sur **DNS**



2) : cliquez-droit sur DNS-SRV (**Server Name**), où nom serveur est le nom du serveur, puis cliquez sur l'onglet Redirecteurs

Rendez-vous âge suivante :



3) : Cliquez sur un nom de domaine DNS Dans la liste de domaine DNS. Ou, cliquez sur Nouveau, tapez le nom du domaine DNS pour lequel vous voulez rediriger les requêtes dans la zone Domaine DNS,

Puis cliquez sur OK.

4) : Dans la boîte IP du domaine sélectionné l'adresse expéditeur, tapez l'adresse IP du premier serveur DNS vers lequel vous souhaitez transférer, puis cliquez sur Ajouter. (Ici on rajoute notre serveur DNS)(192.168.156.108)

5) : Répétez l'étape 4 pour ajouter les serveurs DNS vers lequel vous souhaitez transférer, habituellement, vous pouvez avoir deux FAI du serveur DNS,

Cliquez sur OK

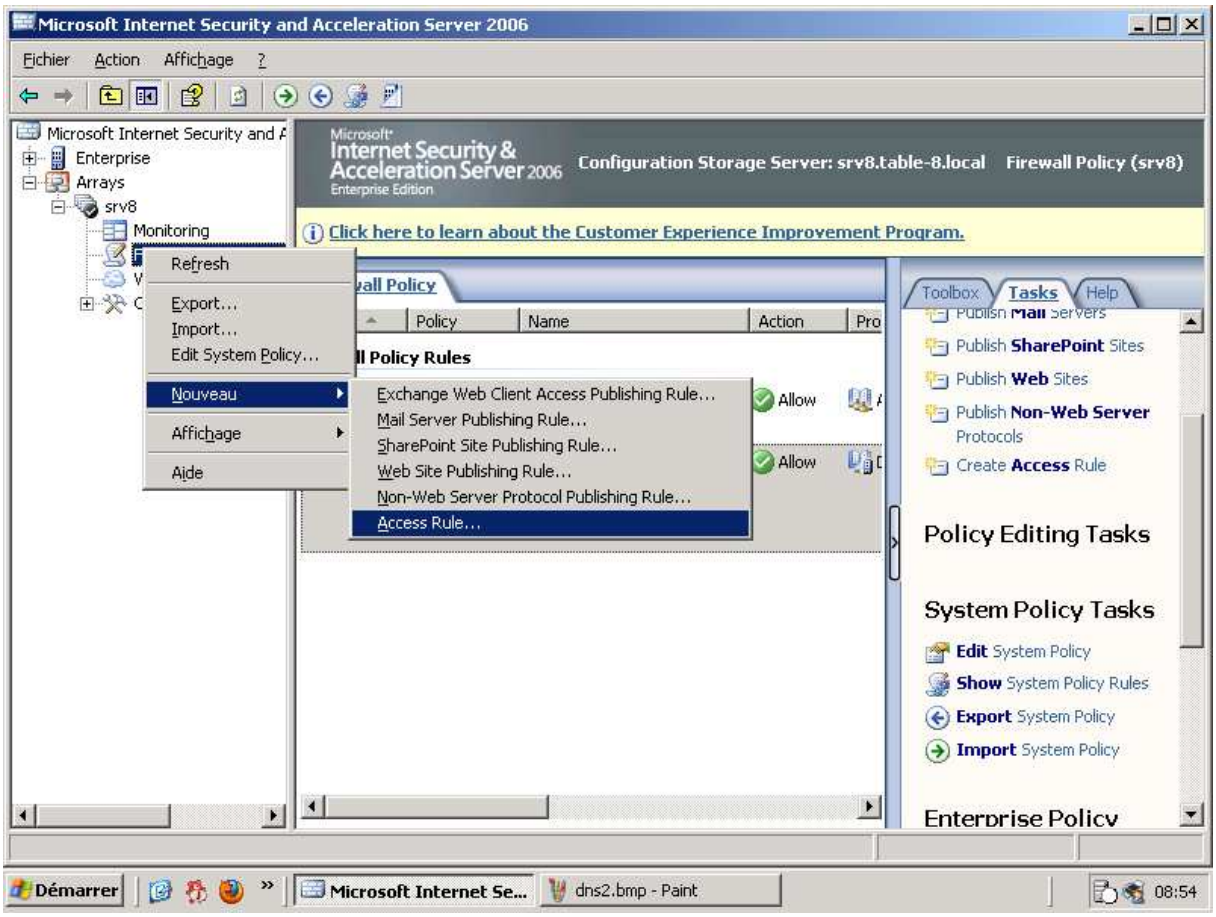
La dernière chose que vous devez faire sur votre serveur DNS est de la définir comme un **client Nat sécurisé**, cela se fait en définissant sa passerelle par défaut à ISA Server IP interne.

C'est tout ce que vous avez à faire sur votre serveur DNS interne, maintenant on va voir ce que nous devons faire avec ISA Server.

La suite, page suivante :

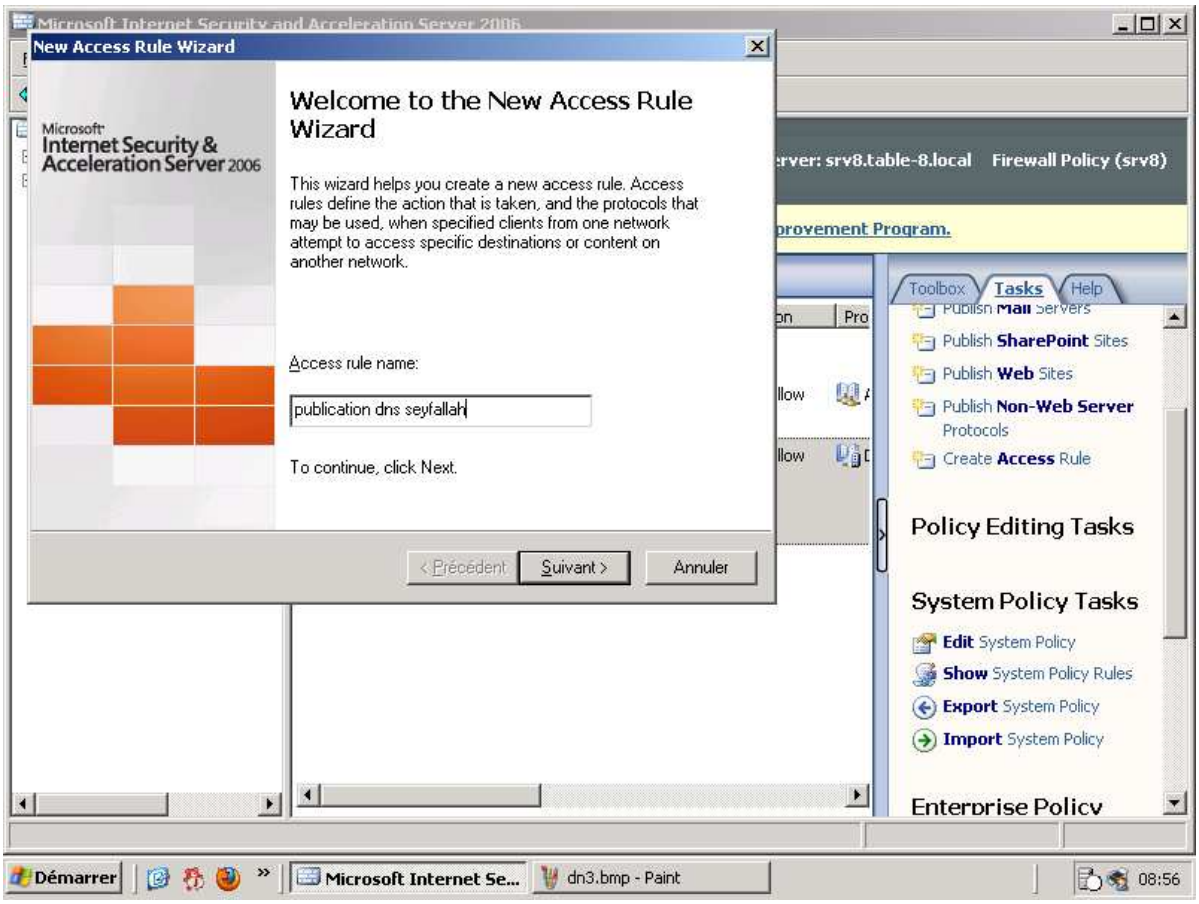
Configuration ISA Server 2006 :

1) Ouvrez **ISA Management Console**
2) Créez une nouvelle règle d'accès, un clic droit sur **Firewall Policy**, puis cliquez sur **Nouveau** puis choisissez **règle d'accès.**



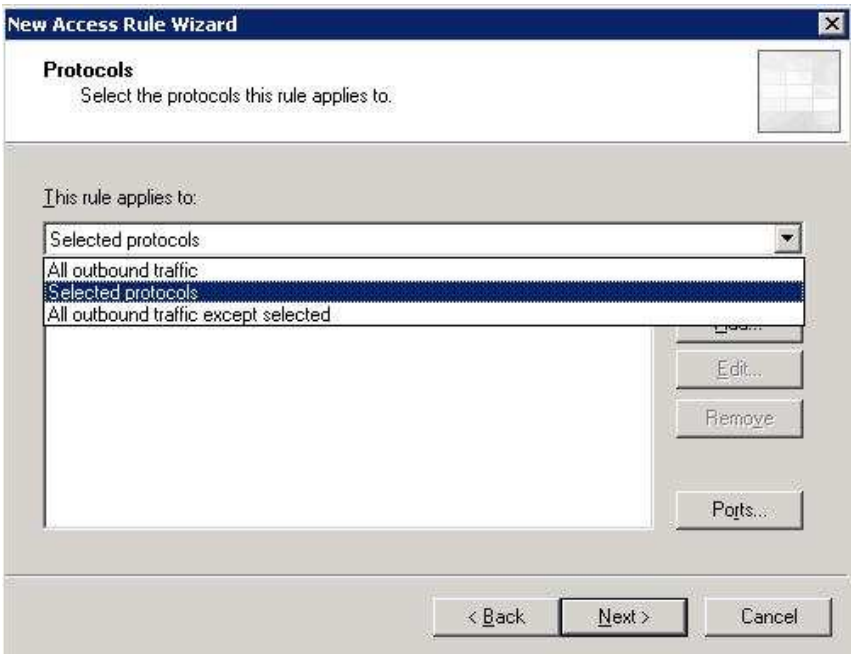
3) L'Assistant Nouvelle règle d'accès seront lancés, donner un nom à votre nouvelle règle, dans cet exemple nous allons mettre le nom (publication DNS seyf Allah).

Suite page suivante.

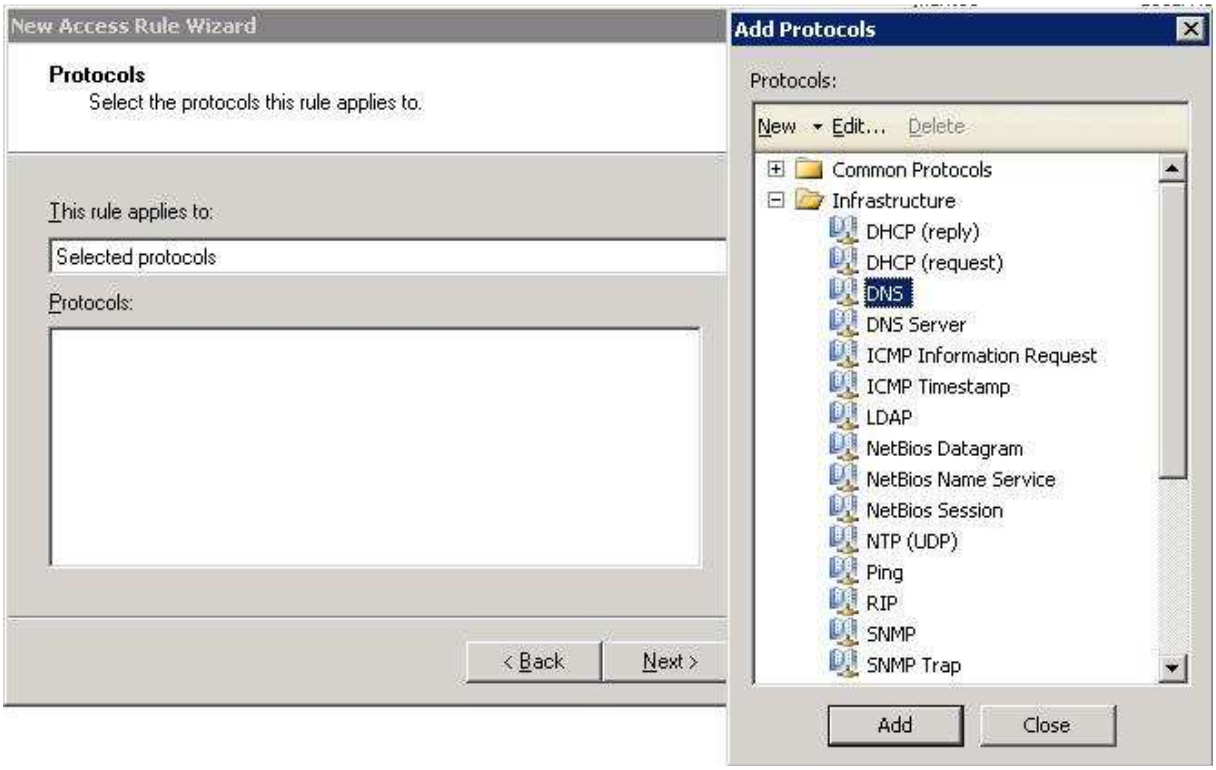


4) Dans la page **Action de la règle,** cliquez sur **Autoriser,** puis cliquez sur **Suivant**

5) Dans la page de **protocoles,** à partir de la liste déroulante sélectionnez **Protocoles sélectionnés** :



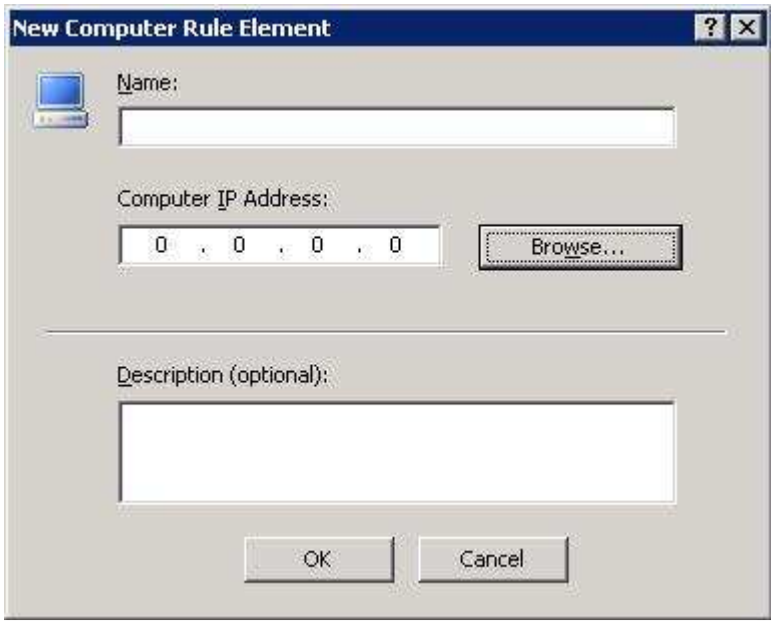
Ensuite cliquez sur le bouton ajouter.et choisissez le protocole DNS.



Le protocole sélectionné sera affiché dans la page Protocoles, cliquez sur Suivant

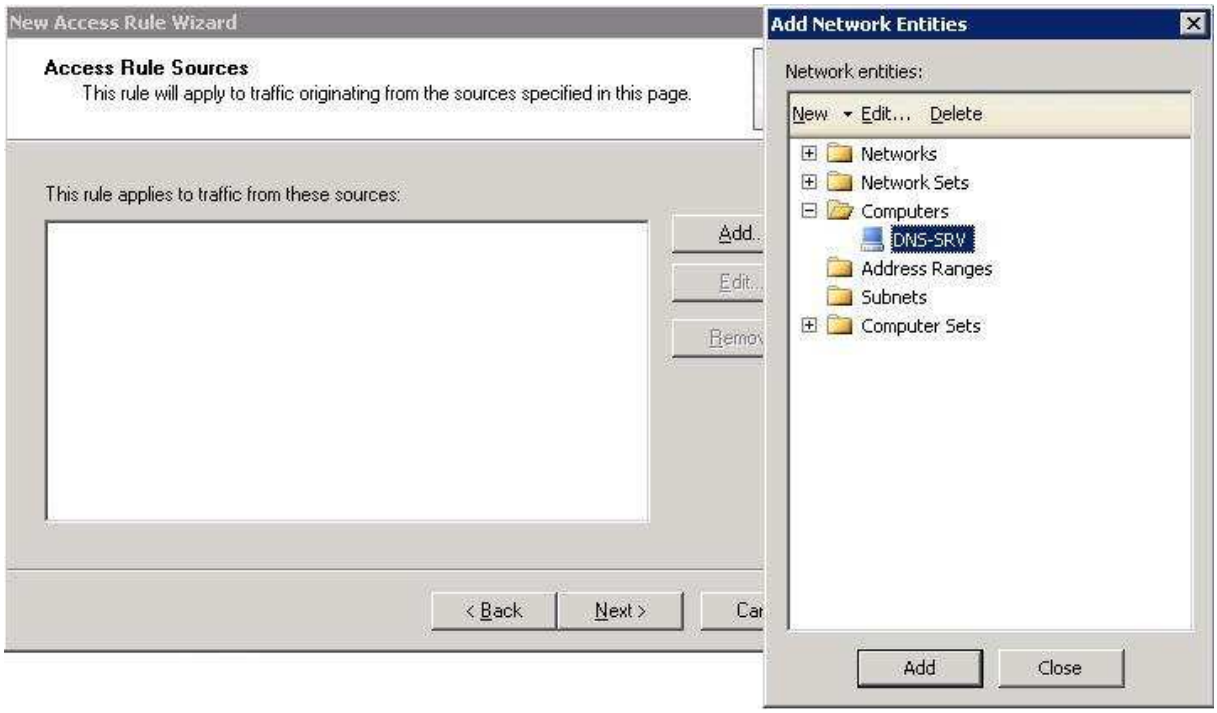
6) Sur la page Sources de règle d'accès, cliquez sur le bouton Ajouter. Ensuite cliquez sur nouveau et ajouter un ordinateur

On a cette page qui s'ouvre .on rentre le nom de l'ordinateur suivi de notre DNS (192.168.156.108)

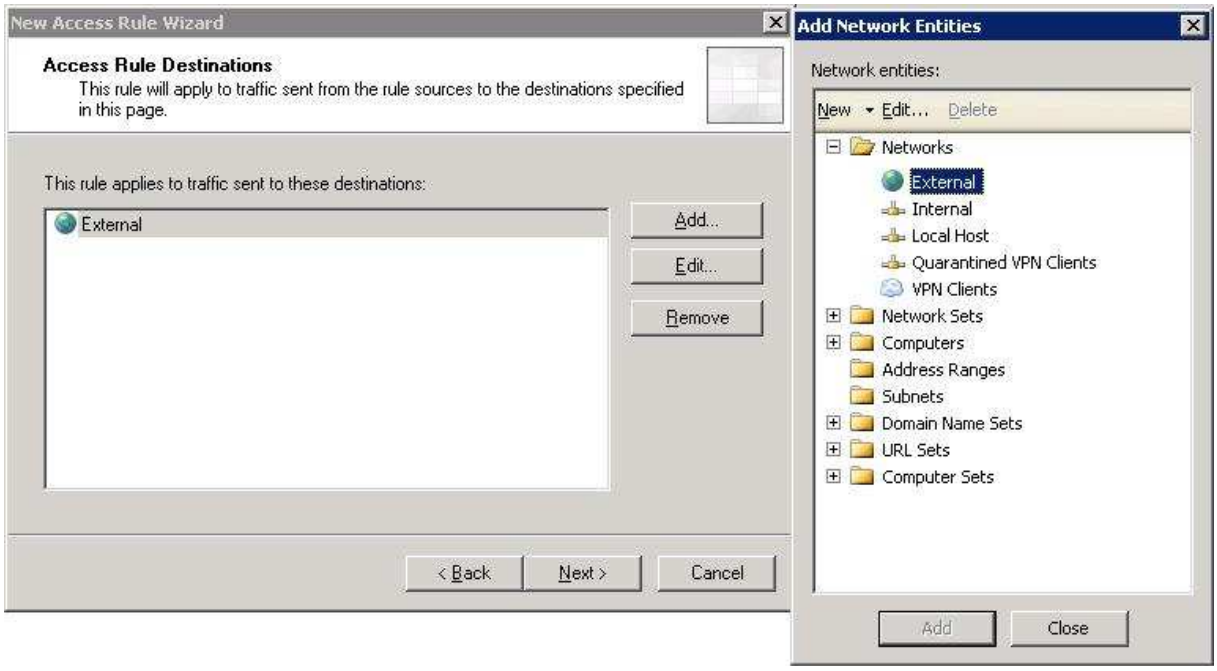


On clique sur ok.

7) Cliquez sur le dossier Ordinateurs. Double-cliquez sur le **DNS-SRV**, puis cliquez sur le bouton Fermer dans la zone Ajouter des entités réseau boîte de dialogue. Click Next in the Access Rule Sources dialog box. Cliquez sur Suivant dans les sources de règle d'accès à la boîte de dialogue.

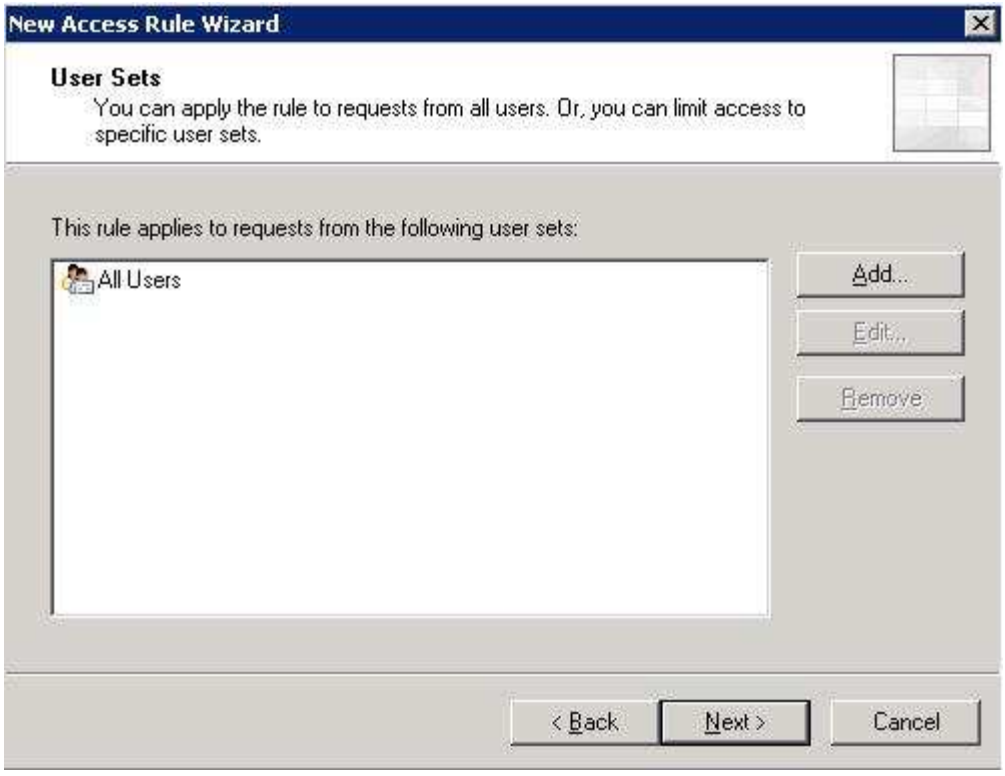


Une fois qu'on a cliqué sur NEXT on va avoir la fenêtre suivante :



8) Donc ici on clique sur ADD (ajouter) et on sélectionne le réseau **(External)=externe**
On ferme la fenêtre et on clique sur Next.

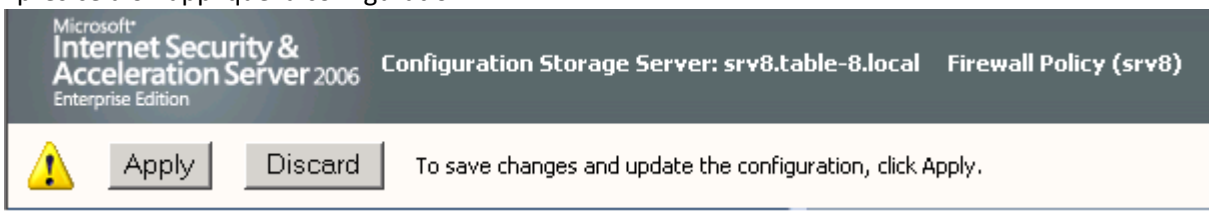
9) Sur la page suivante on laisse par défaut (**tous les utilisateurs.)**



Et on clique sur Next.

On vérifie nos paramètres et on clique sur terminé

Après cela on applique la configuration :



Voici ma règle (DNS)

Une fois la règle créé il faut maintenant créer une règle pour permettre aux utilisateurs de surfer sur internet, commencer à créer une nouvelle règle d'accès comme précédemment

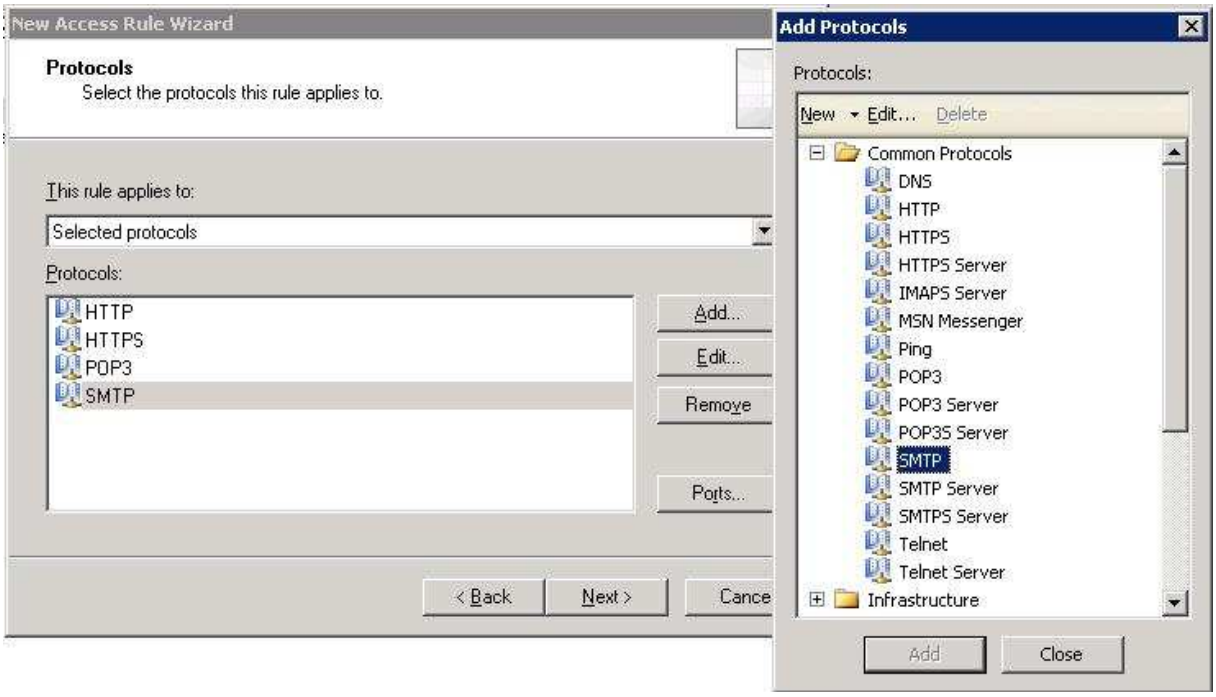
1) clique droit sur Firewall Policy, puis cliquez sur Nouveau puis cliquez sur Règle d'accès

2) Nommez cette règle **allow internet** puis cliquez sur **suivant**

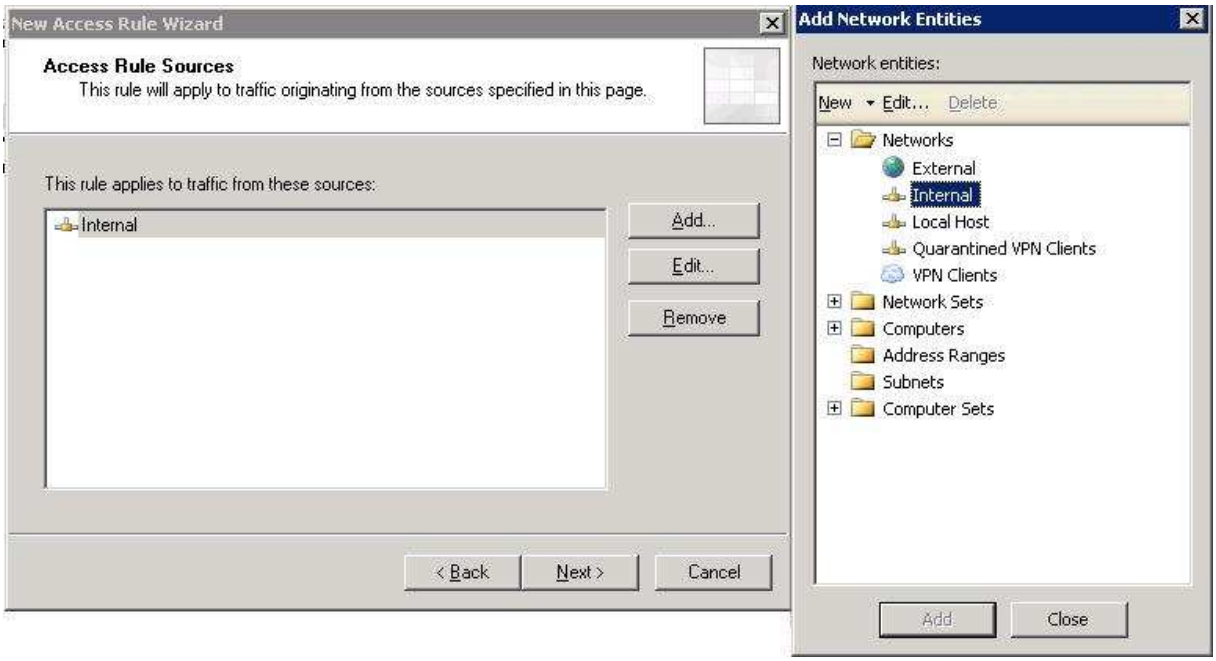
3) Dans la page **Action de la règle,** cliquez sur **Autoriser,** puis cliquez sur **Suivant**

4) Dans la page des protocoles sélectionner les protocoles suivant :

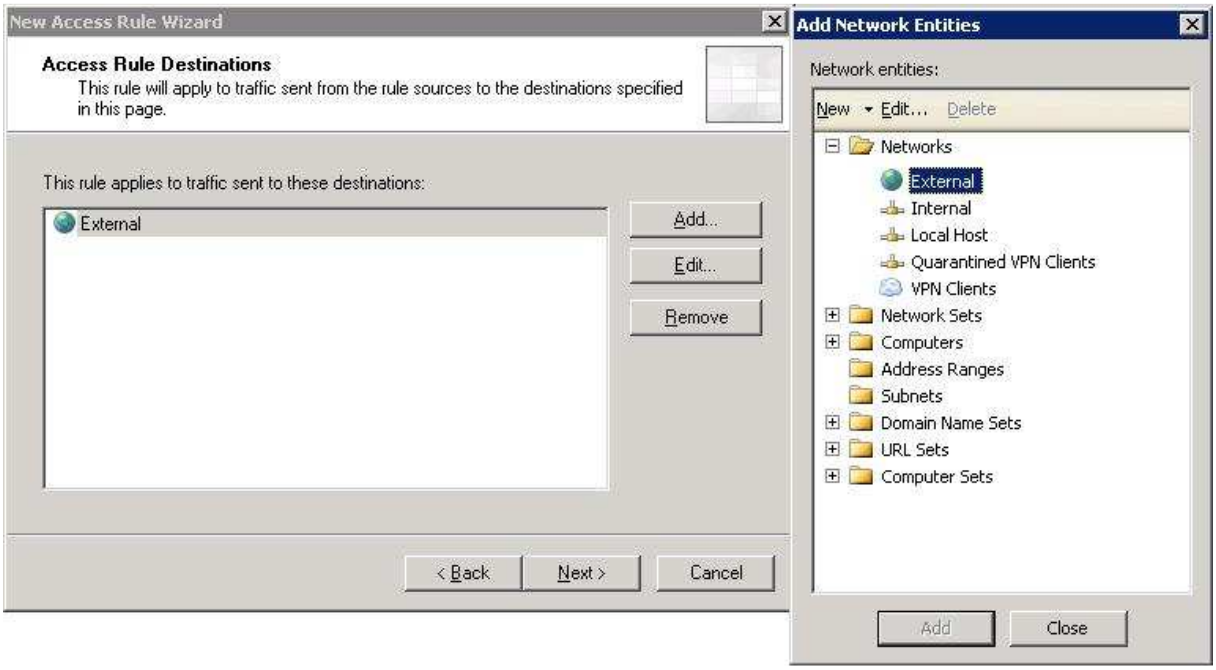
HTTP, HTTPS, POP3 et SMTP. Cliquez sur **Ajouter dans** chaque Protocol. Le protocole de votre choix et une fois que vous ajouté ces Protocoles Cliquez sur **Fermer.**
Puis cliquez sur **Suivant (regardez l'image que j'ai pris pour mieux expliquer.)**



5) Sur cette page de règle d'accès Dans la page **Ajouter des entités réseau** boîte de dialogue, cliquez sur le dossier **Networks.** Double-cliquez sur le réseau **internal,** puis cliquez sur le bouton **Fermer** dans la zone **Ajouter des entités réseau** boîte et cliquez sur suivant.



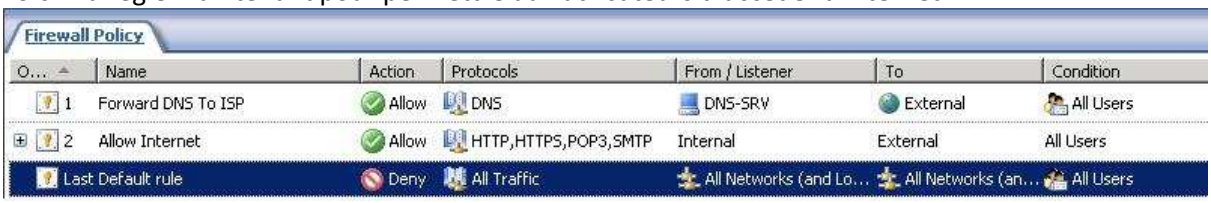
6) Sur cette page de règle d'accès Dans la page **Ajouter des entités réseau** boîte de dialogue, cliquez sur le dossier **Networks.** Double-cliquez sur le réseau **external,** puis cliquez sur le bouton **Fermer** dans la zone **Ajouter des entités réseau** boîte et cliquez sur suivant.



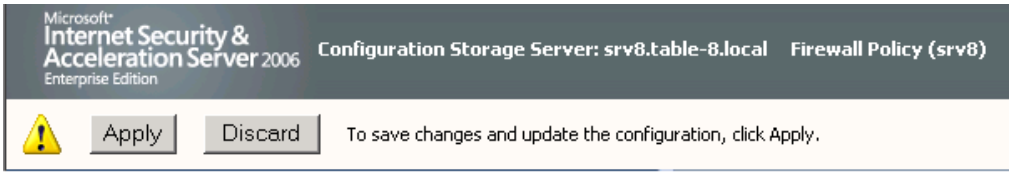
7) Sur la page **Ensembles d'utilisateurs**, acceptez le paramètre par défaut de **tous les utilisateurs.**

8) Vérifiez vos paramètres et cliquez sur Terminer dans la fenêtre Fin de l'Assistant Accès à la page Nouvelle règle.

9) Voici ma règle maintenant pour permettre aux utilisateurs d'accéder à internet.



10) Après cela on applique la configuration.



Cliquez sur le bouton Appliquer pour enregistrer les modifications et actualiser la politique de pare-feu.

Voila **la publication DNS** est fini, maintenant le client pourra aller sur internet sans qu'il et besoin de mettre le DNS du FAI, **il faudra qu'il mette le DNS du serveur qui se trouve dans son réseau c'est a dire ici dans le réseau de table -8 le DNS suivant : 192.168.156.108**

Dans cet article, je vous ais appris à configurer votre serveur DNS interne de transmettre la demande à des serveurs DNS de votre FAI, et également appris à créer la règle nécessaire pour permettre à ISA afin de permettre la communication entre le DNS interne et le DNS FAI.