MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II en Electronique

Option : Réseaux et télécommunication

Thème :

Mise en œuvre d'une infrastructure réseau sécurisée par le ISA Server

Proposé et dirigé par :

Mr. R.ZIANI

Mr. M.KIBOUH

Présenté par :

M^{elle}. YADDADENE Farida

M^{elle}. TOUMI Nedjma

Année universitaire 2011/2012

Remerciements

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

Nous tenons à exprimer nos plus sincères remerciements à notre promoteur Mr.ZIANI qui nous a aidées tout au long du travail.

Un grand merci à notre Co-promoteur Mr.KIBOUH pour ses encouragements et ses orientations qui nous ont beaucoup aidées au cours de notre projet.

Nos remerciements les plus vifs s'adressent aussi à messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de Notre cycle universitaire.

Un grand merci également à nos familles et nos amis pour leurs aides considérables.

Dédicaces

Je dédie ce travail

- *A mes très chers parents, pour leurs sacrifices et leurs dévouements pour mon bonheur. Que Dieu les garde*
- *A mes chers frères et mes chères sœurs*
- *A mes chères nièces et mes chers neveux*
- *A toute ma promotion Master II*
- *A tout mes amis (es)*
- *A tous ceux qui me sont chers*

Farida

Dédicaces

Je dédie ce travail

- *A mes très chers parents, pour leurs sacrifices et leurs dévouements pour mon bonheur. Que Dieu les garde*
- *A mes chers frères et mes chères sœurs*
- *A toute ma promotion Master II*
- *A tout mes amis (es)*
- *A tous ceux qui me sont chers*

Nedjma

Sommaire

CHAPITRE II : Le ISA Server

CHAPITRE III : Mise en œuvre d'une infrastructure réseau sécurisée par le ISA Server

Sommaire

Liste des figures

Liste des tableaux

Introduction générale

Introduction générale

Un réseau informatique est un maillage de micro-ordinateurs interconnectés dans le but d'assurer le transfert de fichiers, le partage des ressources (imprimantes et données), l'exploitation de la messagerie ou l'exécution et la maintenance des programmes à distance. Quel que soit le type de systèmes informatiques utilisés au sein d'une entreprise, leur interconnexion pour constituer un réseau est aujourd'hui indispensable. Les objectifs d'un réseau sont multiples, comme le partage des ressources informatiques entre les différents partenaires de l'entreprise (salariés, dirigeants, fournisseurs, etc …) et la transmission plus rapide des informations.

Aujourd'hui les entreprises utilisent de plus en plus d'informations, ce qui nécessite une meilleure organisation et des conditions de stockage optimales. L'outil informatique joue un rôle primordial sur ce plan. Pour faciliter la transmission de ces données informatisées, les entreprises s'organisent autour d'un réseau.

Avec le développement de l'utilisation d'internet, de plus en plus les entreprises ouvrent leur système d'information à des utilisateurs externes (partenaires, fournisseurs, membres de l'administration) au réseau local, il est dont essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur Internet.

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines. Vu l'expansion et l'importance grandissante des réseaux informatiques, lesquels réseaux ont engendré le problème de sécurité des systèmes d'information; Dans la plupart d'organisations informatisées, partager les données directement entre machines est leur souci majeur. Il s'avère indispensable de renforcer les mesures de sécurités, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Afin d'assurer un bon fonctionnement global de l'entreprise, on utilise une passerelle puissante et facile à administrer qui fournisse une connexion sécurisée tout en augmentant et améliorant les performances réseaux. ISA Server répond à ces exigences par la solution de connectivité Internet et le contrôle d'accès.

Introduction générale

Notre mémoire est réparti en trois chapitres, le premier chapitre présente des généralités sur les réseaux informatiques et les critères de la sécurité des réseaux, dans le deuxième chapitre nous exposerons le principe de fonctionnement du pare-feu ISA Server, le troisième chapitre sera consacré à l'installation et la configuration du ISA server dans le but de sécuriser notre infrastructure réseau.

Et enfin, nous terminerons notre mémoire par une conclusion générale ainsi que des perspectives ouvertes.

Chapitre I

La sécurité des réseaux informatiques

I.1 Introduction

L'informatique est devenue un outil incontournable de gestion, d'organisation, de production et de communication. Le réseau informatique de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises ou personnes ou les importe à partir d'autres sites. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Vu l'importance des informations qui sont souvent véhiculées dans les réseaux, ceux-ci requièrent un certain degré de sécurité. Toutefois le constat est que ceux qui font usage des réseaux ignorent parfois les risques auxquels ils sont exposés lorsqu'une mesure de sécurité n'est pas mise en place. Les réseaux les plus sécurisés disposent très souvent d'un outillage matériel et logiciel afin d'assurer une sécurité optimale.

I.2.Généralités sur les réseaux informatiques

I.2.1.Définition d'un réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et périphériques connectés les uns aux autres afin d'assurer des échanges informatiques tel que le transfert des fichiers, le partage de ressources (imprimantes et données), la messagerie ou l'exécution de programmes à distance.

Le terme réseau peut désigner plusieurs choses en fonction de son contexte :

- désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qui est le cas lorsqu'on parle de l'Internet.
- décrire la façon dont les machines d'un site sont interconnectées
- spécifier les protocoles qui sont utilisés pour que les machines communiquent.

Networking : Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources.

On appelle nœud (node) l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions (un ordinateur, un routeur, un concentrateur, un commutateur).

I.2.2.Les avantages de la mise en réseau

Un réseau informatique a plusieurs buts distincts :

- ✓ Partage des ressources logicielles (Applications).

- ✓ Partage des ressources matérielles (Imprimantes).
- ✓ Partage des données.
- ✓ Communication entre personnes distantes.
- ✓ Communication entre processus (Machines industrielles).
- ✓ Diminuer les coûts.
- ✓ Organisations efficaces.
- ✓ Accès aux données en temps réel.

I.2.3.Classification des réseaux

I.2.3.1Classification selon l'étendue

En fonction de la localisation, de la distance et du débit, les réseaux sont classés en trois types:

- **LAN (Local Area Network)**

Réseau local, intra entreprise permettant l'échange de données et le partage de ressources. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

La vitesse de transfert de données d'un réseau local varie entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

- **MAN (Metropolitain Area Network)**

Réseau métropolitain qui permet la connexion de plusieurs sites à l'échelle d'une ville. Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kms). Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

Dans un MAN on trouve des commutateurs ou des routeurs interconnectés par des liens hauts débits (en général en fibre optique).

- **WAN (Wide Area Network)**

Réseau à l'échelle d'un pays, généralement celui des opérateurs. Le plus connu des WAN est Internet.

Un WAN (ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance).

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

I.2.3.2.Classification selon la topologie (méthode d'accès)

- **La topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau, elle désigne le fait que lors de l'émission de données sur le bus par une station de travail, l'ensemble des stations de travail connectées sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopie.

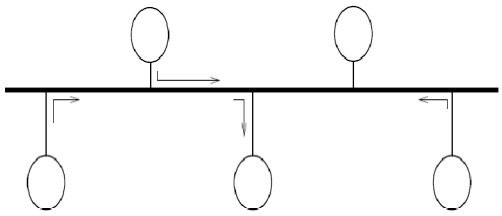


Figure I.1 : topologie en bus

Cette topologie a comme avantage d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

➢ La topologie en anneau

L'information circule le long de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie.

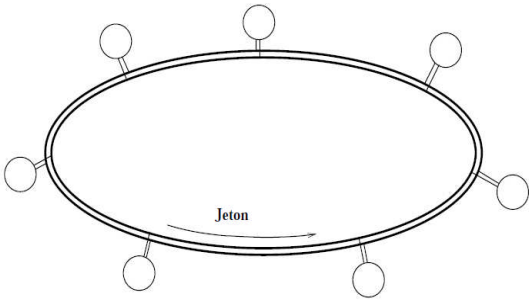


Figure I.2 : topologie en anneau

Dans cette topologie chaque ordinateur joue le rôle d'un répéteur en générant de nouveau le signal avant de le transmettre à l'ordinateur suivant, mais tout l'anneau doit être réinitialisé après chaque problème.

➢ La topologie en étoile

L'ensemble des stations de travail est connecté à un concentrateur qui examine le contenu du message, le régénère et ne le transmet qu'à son destinataire. C'est en réalité un réseau de "n" liaisons point par point, car il établit un circuit entre une paire d'utilisateurs.

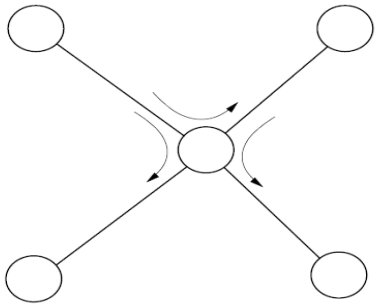


Figure I.3 : Topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.

En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire.

I.2.3.3.Classification selon l'organisation

➢ Egale à égale (Peer to Peer)

Les postes de travail sont simplement reliés entre eux par le réseau. Aucune machine ne joue un rôle particulier. Chaque poste peut partager ses ressources avec les autres postes. C'est à l'utilisateur de chaque poste de définir l'accès à ses ressources. Il n'y a pas obligatoirement d'administrateur attitré, donc chaque poste est à la fois serveur et client. Ce type de réseau n'offre de réel intérêt que dans une configuration particulière dont les postes sont peu nombreux (pas plus d'une dizaine), et les utilisateurs restent attachés à un poste dont ils sont responsables.

✓ Les avantages

• Il est facile de mettre en réseau des postes qui étaient au départ isolés.
• Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.
• Dans un groupe de travail, l'imprimante peut être utilisée par tous.
• Cette méthode est pratique et peu coûteuse pour créer un réseau domestique.

✓ Les inconvénients

• Chaque utilisateur a la responsabilité du fonctionnement du réseau.
• Les outils de sécurité sont très limités.
• Si un poste est éteint ou s'il se "plante", ses ressources ne sont plus accessibles.
• Le système devient ingérable lorsque le nombre de postes augmente.
• Lorsqu'une ressource est utilisée sur une machine, l'utilisateur de cette machine peut voir ses performances diminuer.

➢ Client/serveur

Ce type de réseau est le plus performant et le plus fiable. C'est ce type d'architecture que l'on retrouve sur les réseaux d'entreprise, qui peut parfaitement supporter plusieurs centaines de clients, voire plusieurs milliers.

✓ **Les avantages**

• Les serveurs sont conçus pour le partage de ressources et ne servent pas de station de travail. Il suffit de les dimensionner en fonction de la taille du réseau et du nombre de clients susceptibles de s'y connecter.

• Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "Peer to Peer".

• Ils proposent également des fonctions avancées à l'usage des utilisateurs comme par exemple les profils itinérants qui permettent à un utilisateur (sous certaines conditions) de retrouver son environnement de travail habituel, même s'il change de poste de travail.

• Les serveurs étant toujours en service (sauf en cas de panne...), les ressources sont toujours disponibles pour les utilisateurs.

• Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en œuvre.

✓ **Les inconvénients**

• La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste", et le coût est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.

• Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.

• Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer le fonctionnement en cas de panne.

I.2.4.La communication sur un réseau

La transmission d'information entre 2 programmes informatiques sur 2 machines différentes passe par deux modèles: le modèle OSI ou le modèle TCP/IP. Ces deux normes permettent à chaque partie de la communication de dialoguer. Chaque modèle inclut plusieurs couches. Le terme couche est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs niveaux de protocoles.

L'intérêt d'un modèle en couches est de séparer le problème en différentes parties selon leur niveau d'abstraction. Ainsi, chaque couche du modèle communique avec une couche adjacente, utilise les services de couches inférieures et fournit des services à la couche de niveau supérieur.

I.2.4.1.Le modèle OSI

OSI (Open System Interconnections), est un modèle de base qui a été défini par l'ISO (International Standard Organisation). Cette organisation revient régulièrement pour mettre en place un standard de communications entre les ordinateurs d'un réseau. En effet, aux origines des réseaux chaque constructeur avait un système propre et de nombreux réseaux incompatibles coexistaient. Ce modèle a permis de standardiser la communication entre les machines afin que les différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles. Ce modèle définit 7 niveaux différents pour le transport de données.

Modèle OSI	
Niveau	**couche**
Niveau 7	Couche application
Niveau 6	Couche présentation
Niveau 5	Couche session
Niveau 4	Couche transport
Niveau 3	Couche réseau
Niveau 2	Couche liaison de données
Niveau 1	Couche physique

Tableau I.1 : le modèle OSI

Niveau 1: la couche physique, gère les connections matérielles, définit la façon dont les données sont converties en signaux numériques sur le média de communication.

Niveau 2: la couche liaison de données, définit l'interface avec la carte réseau, et le partage du média de transmission.

Niveau 3: la couche réseau, gère l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.

Niveau 4: la couche transport, gère la remise correcte des informations (gestion des erreurs), et assure le contrôle de l'acheminement.

Niveau 5: la couche session, s'occupe de l'établissement, de la gestion et de la coordination des communications, elle définit l'ouverture et la destruction des sessions de communication entre les machines du réseau.

Niveau 6: la couche présentation, s'occupe de la mise en forme des données, éventuellement de l'encryptage et de la compression des données, par exemple mise en forme des textes, images et vidéo.

Niveau 7: la couche application, assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

I.2.4.2.Le modèle TCP/IP

Le modèle TCP/IP est inspiré du modèle OSI. Il fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, mais ne contient, lui, que quatre couches. Ces couches ont des tâches beaucoup plus diverses étant donné qu'elles correspondent à plusieurs couches du modèle OSI.

TCP (Transfert Contrôle Protocole) : se charge du transport de bout en bout pour toute application.

IP (Internet Protocole) : est responsable du routage à travers le réseau.

<table>
<tr><th>Niveau</th><th>Modèle TCP/IP</th><th>Modèle OSI</th><th>Protocoles TCP/IP</th></tr>
<tr><td rowspan="3">Niveau 4</td><td rowspan="3">Couche Application</td><td>Couche Application</td><td rowspan="3">Applications réseau (Telnet, SMTP, FTP…)</td></tr>
<tr><td>Couche Présentation</td></tr>
<tr><td>Couche Session</td></tr>
<tr><td>Niveau 3</td><td>Couche Transport (TCP)</td><td>Couche Transport</td><td>TCP ou UDP</td></tr>
<tr><td>Niveau 2</td><td>Couche Internet (IP)</td><td>Couche Réseau</td><td>IP, ARP, RARP</td></tr>
<tr><td rowspan="2">Niveau 1</td><td rowspan="2">Couche Accès réseau</td><td>Couche Liaison de données</td><td rowspan="2">FTS, FDDI, PPP, Ethernet, Anneau à jeton (Token Ring)</td></tr>
<tr><td>Couche Physique</td></tr>
</table>

Tableau I.2 : le modèle TCP/IP

Niveau 1 : la couche accès réseau, spécifie la forme sous laquelle les données doivent être acheminées quelque soit le type de réseau utilisé.

Niveau 2 : la couche Internet, elle est chargée de fournir les paquets de données (datagramme).

Niveau 3 : la couche Transport, elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission.

Niveau 4 : la couche Application, elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...).

➢ Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

- Le paquet de données est appelé **message** au niveau de la couche application.
- Le message est ensuite encapsulé sous forme de **segment** dans la couche transport. Le message est donc découpé en morceaux avant envoi.
- Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme.**
- Enfin, on parle de **trame** au niveau de la couche accès réseau.

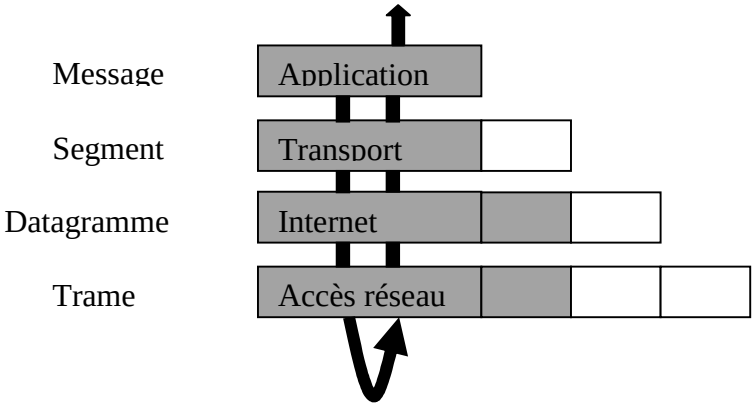


Figure I.4: principe d'encapsulation

I.2.5.Les différents protocoles

Protocole TCP

TCP (Transmission Control Protocol) est l'un des principaux protocoles de la couche transport, créé dans le but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs autonomes et raccordés à un réseau. TCP est un protocole orienté connexion (il permet à deux machines qui communiquent de contrôler l'état de la transmission). Les caractéristiques principales du protocole TCP sont les suivantes :

- Remettre en ordre les datagrammes à l'aide du protocole IP.
- Vérifier le flot de données afin d'éviter une saturation du réseau.
- Formater les données en segments de longueur variable afin de les remettre au protocole IP.
- Faire circuler simultanément des informations provenant de sources distinctes sur une même ligne.
- Permet l'initialisation et la fin d'une communication.

Le protocole UDP

Le protocole UDP (User Datagram Protocol) est comme TCP, un protocole de transport de données. Cependant, contrairement à TCP, on qualifie l'UDP de transmission « en mode non connecté et non fiable » ou encore de protocole « non orienté connexion ».

Ceci signifie simplement que la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première.

Les données sont ainsi envoyées sous forme de bloc (datagramme). Il n'y a pas de contrôle d'erreur.

Protocole IP

Le protocole IP fait partie de la couche internet, c'est l'un des protocoles les plus importants d'internet car il permet l'élaboration et le transport des datagrammes IP, sans toutefois en assurer la livraison. En réalité le protocole IP traite les datagrammes IP indépendamment les un des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire du message grâce à trois champs :

- ✓ Le champ adresse IP : c'est l'adresse de la machine, Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les note sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255.
- ✓ Le champ masque de sous-réseau : un masque de sous-réseau permet au protocole IP de déterminer la partie de l'adresse IP qui concerne le réseau.
- ✓ Le champ passerelle par défaut : il permet au protocole internet de savoir à quelle machine remettre le datagramme si jamais la machine de destination n'est pas sur le réseau local.

Protocole ARP

Le protocole ARP (Address Resolution Protocol) a un rôle important parmi les protocoles de la couche internet de la suite TCP/IP, car il permet de connaitre l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle protocole de résolution d'adresse.

Le protocole ARP interroge les machines du réseau pour connaitre leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache. Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. Les machines du réseau vont comparer cette adresse logique à la leur, si l'une d'entre elle s'identifie à cette adresse, la machine va répondre à ARP qui va stocker le couple d'adresses dans la table de correspondance et la communication va pouvoir avoir lieu.

Protocole RARP

Le protocole RARP (Reverse Address Resolution Protocol) est beaucoup moins utilisé, il signifie protocole ARP inversé, il permet à une station de connaitre son adresse IP à partir d'une adresse table de correspondance entre adresse physique (MAC) et adresse IP hébergée par une passerelle située sur le même réseau.

Protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles. ICMP rapporte les messages d'erreur à l'émetteur initial. Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet : machine destination déconnectée, durée de vie des datagrammes expirée, congestion de passerelles intermédiaires. Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'Internet. Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP.

Le protocole FTP

Le protocole FTP (File Transfer Protocol) définit la façon selon laquelle des données doivent être transférées sur TCP/IP. Le protocole FTP a pour objectifs de :

- Permettre un partage de fichiers entre deux machines distantes.
- Permettre une indépendance aux systèmes de fichiers des machines clientes et serveur.
- Permettre de transférer des données de manière efficace.

Le protocole TELNET

Le protocole TELNET est un protocole standard d'internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Il utilise un modèle client/serveur qui permet d'exécuter des commandes à distance. Il est souvent utilisé pour exécuter des commandes sur un serveur à partir d'un terminal.

Le TELNET est utile non seulement pour récupérer des emails, des informations et des programmes mais également pour l'entretien de site web, et la configuration de routeur à distance. Le serveur TELNET n'est pas sécurisé, toutes les informations (y compris le compte d'utilisateur et le mot de passe) circulent en clair sur le réseau.

Lorsque le protocole TELNET est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.

Le protocole SMTP

Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier d'une machine à une autre. Ce protocole fonctionne en mode connecté, il est par défaut sur le port 25.

Le protocole POP3

Le protocole POP3 (Port Office Protocol version 3) occupe le port 110, il est nécessaire pour les personnes n'étant pas connectées en permanence à internet de pouvoir consulter les mails reçus hors connexion.

I.3.La sécurité des réseaux informatiques

I.3.1.Principe de la sécurité

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.

- **Disponibilité :** demande que l'information sur le système soit *disponible* aux personnes autorisées.
- **Confidentialité :** demande que l'information sur le système ne puisse être *lue* que par les personnes autorisées.
- **Intégrité :** demande que l'information sur le système ne puisse être *modifiée* que par les personnes autorisées.
- **Non répudiation :** permet de garantir qu'une transaction ne peut être niée.
- **Authentification :** garantit l'identité des correspondants ou des partenaires qui communiquent.

I.3.2.Politique de sécurité

La politique ou stratégie de sécurité est un plan d'actions définies par les personnes qui ont accès aux ressources technologiques et aux données vitales de l'entreprise afin de protéger son réseau contre les attaques menées soit de l'intérieur, soit de l'extérieur. Elle a pour objectif :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

I.3.3.Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini :

- **Les vulnérabilités :** ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.
- **Les attaques (exploits):** elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Les contre-mesures :** ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).
- **Les menaces :** ce sont des adversaires capables de monter une attaque exploitant une vulnérabilité.

I.3.4.Les types de menaces

Menaces accidentelles (risques)

Les menaces accidentelles sont celles qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles sont : défaillance de systèmes, fautes opérationnelles et bogues dans les logiciels.

- **Menaces intentionnelles (attaques)**

Une menace intensionnelle est une action exécutée par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources.
Les menaces intentionnelles peuvent être passives ou actives.

- ✓ **Menaces passives** : Les menaces passives sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne changent. Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.
- ✓ **Menaces actives (attaques)** : Les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou du fonctionnement du système. Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable. Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données. Le résultat d'une attaque est soit une divulgation de l'information : violation de la confidentialité de l'objet, soit une modification des objets : violation de l'intégrité de l'objet, soit un déni de service : violation de la disponibilité.

I.3.5.Les techniques d'attaques

I.3.5.1.Attaques de mots de passe

Il existe des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :

- **les keyloggers :** ou «enregistreurs de touches», sont des logiciels qui, lorsqu'ils sont installés sur le poste de l'utilisateur, permettent d'enregistrer les frappes de claviers saisies par l'utilisateur.
- **l'ingénierie sociale :** consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence ;

- **l'espionnage :** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

I.3.5.2.Usurpation d'adresse IP

L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.
La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu). Ainsi, un paquet écouté avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu'un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu.

I.3.5.3.Attaques par déni de service (DoS)

Le déni de service ou DoS (Denial Of Service), est une attaque réalisée dans le but de rendre indisponible durant une certaine période les services ou ressources d'une organisation. Généralement, ce type d'attaque a lieu contre des machines, serveurs et accès d'une entreprise afin qu'ils deviennent inaccessibles pour leurs clients. Le but d'une telle attaque n'est pas d'altérer ou de supprimer des données, ni même de voler quelconque information. Il s'agit ici de nuire à la réputation de sociétés présentes sur Internet en empêchant le bon fonctionnement de leurs activités.

On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles ;
- Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

I.3.5.4.Attaques de l'homme de milieu

L'attaque de l'homme du milieu ou man in the middle attaque (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaquant peut aussi choisir de ne pas réémettre le trafic aspiré et ainsi bloquer toute communication vers l'extérieur, et donc par exemple couper la connexion internet.

La plupart des attaques de types main in the middle consistent à écouter le réseau à l'aide d'outils d'écoute des réseaux.

I.3.5.5.Les virus

Un virus informatique est un programme informatique situé dans le corps d'un autre, qui se répand à travers les ordinateurs et les réseaux en créant ses propres copies, et cela, généralement à l'insu des utilisateurs.

Etant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection. On distingue ainsi différents types de virus :

- **Les vers**

Il s'agit de programmes possédant la faculté de s'auto reproduire et de se déplacer à travers un réseau en utilisant des mécanismes de communication classiques, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager. Un ver est donc un virus réseau.

- **Les bombes logiques**

Elles sont de véritables bombes à retardement. Ce sont de petits programmes restant inactifs tant qu'une condition n'est pas remplie, une fois la condition remplie (une date par exemple), une suite de commandes est exécutée (dont le but, le plus souvent, hélas, est de faire le plus de dégâts possible). Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

- **Les chevaux de Troie**

Un cheval de Troie permet généralement de préparer une attaque ultérieure de la machine infectée. Par exemple, ils agissent en laissant ouverts des ports de communication qui peuvent être ensuite utilisés par des programmes d'attaque. Ils sont difficiles à détecter par un utilisateur non averti. Un cheval de Troie est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté.

Un cheval de Troie peut voler des mots de passe, copier des données sensibles et exécuter toute autre action nuisible.

I.3.6.Les mécanismes de sécurité

I.3.6.1.Les logiciels antivirus

Il s'agit d'un logiciel capable de détecter et de détruire les virus contenus sur un disque. Le logiciel a pour charge de surveiller la présence de virus et éventuellement de nettoyer, supprimer ou mettre en quarantaine le ou les fichiers infectés. Ils surveillent tous les espaces dans lesquels un virus peut se loger, c'est à dire la mémoire et les unités de stockage qui peuvent être locales ou réseau. Le programme est composé de 3 parties ayant chacune un rôle essentiel :

- Un " moteur " qui a pour rôle la détection des virus.
- Une base de données contenant des informations sur les virus connus. C'est cette base de données qu'il faut maintenir à jour le plus régulièrement possible, afin de permettre à l'antivirus de connaître les virus les plus récents.
- Un module de nettoyage qui a pour but de traiter le fichier infecté.

I.3.6.2 La cryptographie

La cryptographie est un ensemble de techniques permettant de transformer les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale. Il existe deux méthodes de cryptage :

- **Le cryptage symétrique**

Le cryptage à clé privée ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et à décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard).

Ce cryptage à un inconvénient, puisqu'il faut que les deux parties possèdent la clé secrète, il faut donc la transmettre d'un bout à l'autre, ce qui est risqué sur un réseau non fiable comme internet car la clé peut ainsi être interceptée.

- **Cryptage asymétrique**

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par l'utilisateur ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par un algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé (la clé publique) est donc utilisée pour le cryptage et l'autre (la clé privée) pour le décryptage.
Ce cryptage présente l'avantage de permettre le placement des signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.
Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons :
- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- Authentification plus flexible.
- Supporte les signatures numériques.

I.3.6.3.Les protocoles de sécurité

Le protocole SSH

Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécurité des informations : la confidentialité. En effet, grâce à ce protocole, il est possible

de chiffrer des données par un système de clés privées et publiques. Ces données transitent dans un « tunnel », une sorte de canal sécurisé où il est impossible de savoir ce qui se passe à l'intérieur.

Dans le protocole SSH, un ordinateur client peut initier une connexion avec un ordinateur serveur et profiter des mesures de sécurité suivantes :

- Après avoir effectué une connexion initiale, le client peut s'assurer de se connecter au même serveur lors des sessions suivantes.
- Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.
- Toutes les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rend extrêmement difficiles à déchiffrer et à lire.

Le protocole SSL

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.….). Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité. Le principe d'une authentification du serveur avec SSL est le suivant :

- Le navigateur du client fait une demande de transaction sécurisée au serveur.
- Suite à la requête du client, le serveur envoie son certificat au client.
- Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- Le client choisit l'algorithme.
- Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- Le navigateur vérifie que le certificat délivré est valide.
- Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

Le protocole Secure HTTP

S-HTTP (http sécurisé) est un procédé de sécurisation des transactions HTTP utilisé pour la navigation sécurisée sur le WWW**.** Il offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web. Pour garantir cette sécurité, S-HTTP fait usage de méthodes de cryptographie asymétrique pour l'authentification et de méthodes de cryptographie symétrique pour le chiffrement des échanges.

Contrairement à SSL qui se trouve au niveau de la couche transport, S-HTTP procure une sécurité basée sur des messages au dessus du protocole HTTP, en marquant individuellement les documents html à l'aide de certificat.

Ainsi, alors que SSL est indépendant de l'application utilisée et crypte l'intégralité de la communication, S-HTTP est très fortement lié au protocole http et crypte individuellement chaque message.

Les messages S-HTTP sont basés sur trois composantes :

- Le message HTTP.
- Cryptographie de l'envoyeur.
- Cryptographie du destinataire.

Ainsi, pour décrypter un message S-HTTP, le destinataire du message analyse les entités du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message.

SSL permet de sécuriser la connexion internet tandis que s-http permet de fournir des échanges HTTP sécurisé.

I.3.6.4.Les réseaux privés virtuels (VPN)

Le VPN permet de relier deux réseaux distants à travers Internet. Il est ainsi possible de faire communiquer ces deux réseaux comme s'ils étaient connectés directement ensemble. Dans le quasi totalité des implémentations d'un VPN, un cryptage est rajouté entre les deux connectiques qui vont initier le VPN.

Les réseaux VPN reposent sur un protocole appelé « tunneling » qui permet de faire circuler les informations de façon cryptée d'un bout à l'autre du tunnel.

Le principe du tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite la source chiffre les données et les achemine en empruntant ce chemin virtuel.

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur :** seuls les utilisateurs autorisés doivent avoir accès au canal virtuel.
- **Cryptage des données :** lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.
- **Gestion des clés :** les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- **Prise en charge multi-protocole :** la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

I.3.6.5.Les pare-feux (firewall)

Un firewall ou pare-feu est un dispositif physique (matériel) ou logique (logiciel) servant de système de protection pour les ordinateurs domestiques. Il peut également servir d'interface entre un ou plusieurs réseaux d'entreprise afin de contrôler et éventuellement bloquer la circulation des données en analysant les informations contenues dans les flux de données.

Rôles d'un pare-feu :

- Contrôler le trafic sortant d'un réseau, et notamment éviter que les utilisateurs accèdent à certains nœuds du réseau.
- Sécuriser le trafic entrant d'un réseau, et empêcher certains nœuds extérieurs de se connecter au réseau local.
- Eviter que certaines machines mal configurées du réseau local n'envoient des données vers l'extérieur.

➢ Principe de fonctionnement

L'architecture la plus en vogue actuellement est basée sur une « **zone démilitarisée** » communément appelée DMZ (Demilitarized zone).

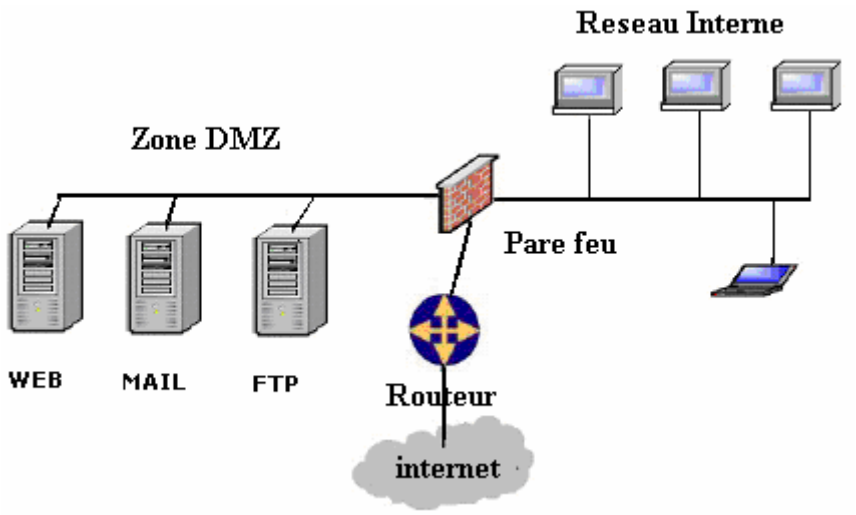


Figure I.5 : le pare feu

Elle consiste à placer un réseau intermédiaire entre l'accès Internet et le réseau interne (éventuellement plusieurs). Cette DMZ sera isolée, aussi bien vis à vis de l'Internet que du réseau local, par des systèmes de filtrage (filtres de paquets). Ensuite, les éventuels serveurs nécessaires à l'entreprise devant continuer à être accessibles de l'extérieur seront connectés directement sur cette DMZ, de manière à les séparer du réseau interne, Par exemple, on pourra y trouver un serveur Web, un serveur DNS, un serveur de mails, un serveur FTP...

Dans le cas où l'un de ces serveurs serait compromis, le filtrage entre la DMZ et le réseau interne doit être capable en plus d'assurer une protection suffisante.

Bien évidemment, cette architecture doit être adaptée plus précisément à la structure d'une entreprise précise, et éventuellement intégrer des composants supplémentaires, tels que des proxys et autres dispositifs.

- **Les différents types de filtrages**

Le filtrage simple de paquet

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le pare-feu ou le routeur par des règles de filtrage, généralement appelées des ACL (Access Control Lists).

Le filtrage dynamique

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au pare-feu. Le pare-feu prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DoS.

Avec le filtrage simple de paquets, il est impossible de prévoir les trafics à laisser passer ou à interdire. Par contre le système de filtre dynamique permet d'effectuer un suivi des transactions et des échanges entre le client et le serveur, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer des règles de filtrage. De cette manière lorsqu'une machine autorisée initie une connexion vers une autre machine située de l'autre coté du pare-feu ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu. Le filtrage dynamique ne protège pas l'exploitation des failles applicatives liées aux vulnérabilités des applications.

Le filtrage applicatif

Le filtrage applicatif (pare-feu de type proxy) est réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

I.4.Conclusion

La connexion d'un réseau à Internet peut exposer une organisation à divers problèmes de sécurité. Des mesures de sécurité et des technologies appropriées doivent être mises en œuvre pour éviter les virus informatiques, les attaques de pirates et l'utilisation frauduleuse des réseaux et des ressources privées, bien qu'aucune mesure de sécurité individuelle ne puisse garantir une protection absolue.

Chapitre II

Le ISA Server

II.1 Introduction

Face à 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 en 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.

II.2 Présentation d'ISA server

Microsoft ISA (*Internet Security and Acceleration*) Server est conçu pour répondre aux besoins des entreprises qui disposent d'un accès à Internet. ISA Server comprend des fonctionnalités de mise en cache qui permettent aux entreprises d'économiser de la bande passante réseau et qui fournissent aux utilisateurs un accès plus rapide au Web. ISA Server dispose également d'un service de pare-feu qui protège les ressources réseau des accès non autorisés provenant de l'extérieur du réseau de l'entreprise, tout en permettant des accès autorisés efficaces. ISA Server comprend des fonctionnalités de gestion et d'administration grâce auxquelles les entreprises peuvent contrôler et gérer l'utilisation et l'accès à Internet d'une manière centralisée. Le ISA server fonctionne dans les couches 3 à 7 de modèle OSI.

II.2.1 Les éditions d'ISA server

ISA Server est disponible en deux éditions conçues pour répondre aux besoins des entreprises en termes d'organisation et de réseau.

- **ISA server édition entreprise**

ISA Server Edition Entreprise est un produit Microsoft combinant un pare-feu d'entreprise et un serveur de cache Web évolutifs. L'Edition Entreprise est conçue pour répondre aux besoins de performances, de gestion et d'évolutivité des environnements Internet à fort trafic, avec une gestion centralisée des serveurs, des stratégies d'accès à plusieurs niveaux et des capacités de tolérance aux pannes. ISA Server Edition Entreprise offre aux environnements stratégiques de l'entreprise une connectivité Internet fiable, évolutive et rapide.

- **ISA server édition standard**

ISA Server Edition Standard apporte des capacités de pare-feu et de cache Web de classe entreprise aux environnements de petite société, de groupe de travail et de département. L'Edition Standard offre aux environnements stratégiques une sécurité robuste, un accès rapide au Web, une gestion intuitive et un excellent rapport performances/prix.

- **La différence entre les deux éditions**

Les caractéristiques de sécurité de cache, de gestion et de performances sont identiques pour les deux éditions. L'Edition Standard est cependant limitée à un serveur autonome, une stratégie locale et quatre processeurs au maximum. L'Edition Entreprise prend en charge les grappes de serveurs avec une gestion centralisée, les stratégies d'entreprise, et les matériels sans aucune limitation.

II.2.2 Les avantages d'ISA server

ISA Server est un outil clé de la famille NET Enterprise Servers. Cette famille regroupe l'ensemble des applications serveur Microsoft qui permettent de créer, déployer et gérer des solutions et des services Web évolutifs et intégrés. ISA Server présente plusieurs avantages pour les entreprises désireuses de connexions Internet rapides, sécurisées et faciles à gérer.

➢Connexion Internet sécurisée grâce à un pare-feu multicouche

La connexion de réseaux et d'utilisateurs à Internet soulève des questions de sécurité et de productivité. ISA Server apporte à l'entreprise des capacités complètes de contrôle d'accès et de surveillance d'utilisation. ISA Server protège les réseaux contre les accès frauduleux, inspecte le trafic et alerte les administrateurs en cas d'attaque.

ISA Server comprend un pare-feu d'entreprise multicouche extensible, garantissant la sécurité du trafic au niveau paquet, circuit et application, le contrôle d'état, le support d'application étendu, le VPN (réseau privé virtuel) intégré, le renforcement du système, la détection intégrée des intrusions, le filtrage d'application intelligent, la transparence pour tous les clients, l'authentification avancée, la publication serveur sécurisée, etc. ISA Server

permet :

- De protéger les réseaux contre les accès frauduleux.
- De défendre les serveurs Web et les serveurs de messagerie contre les attaques externes.
- D'inspecter le trafic réseau entrant et sortant pour garantir la sécurité.
- D'être alerté en cas d'activité suspecte.

➢ Accès rapide à Internet et cache très performant

Internet peut offrir aux organisations des gains de productivité séduisants, sous réserve que l'accès au contenu soit rapide et économique. Avec son cache Web, ISA Server peut réduire au minimum les goulets d'étranglement et les ressources du réseau en bande passante, en servant localement des contenus Web stockés en cache. ISA Server permet :

- De fournir aux utilisateurs un accès Web plus rapide en servant les objets localement plutôt que par l'intermédiaire d'un réseau Internet surchargé.
- De réduire les coûts de bande passante en diminuant le trafic sur le réseau.
- De servir les contenus Web les plus demandés depuis le cache afin de libérer de la bande passante pour les autres demandes.

➢ Gestion unifiée grâce à l'administration intégrée

En associant des fonctions de pare-feu d'entreprise et de cache Web hautes performances, ISA Server constitue une infrastructure de gestion commune qui réduit la complexité et les coûts du réseau. Soit le déployer en tant que système intégré ou sous forme de pare-feu et de cache séparé, il permet de bénéficier d'une gestion intégrée. ISA Server 2006 s'intègre étroitement à Windows 2003, offrant une approche cohérente et puissante pour gérer les accès utilisateur, la configuration et les règles. ISA Server permet :

- D'appliquer des stratégies homogènes au pare-feu et au cache.
- De contrôler les accès par utilisateur, application, type de contenu et agenda.
- De réduire la complexité et les coûts du réseau.
- D'appliquer des règles stratégiques au niveau de l'entreprise.
- De superviser l'utilisation et les performances du réseau.

- De bénéficier de l'intégration à Windows 2003, incluant la sécurité, le VPN, le contrôle de la bande passante avec QoS et le service Active Directory.

➢ Plate-forme extensible et ouverte

ISA Server présente les avantages énumérés ci-dessous en matière d'extensibilité et de personnalisation.

- Il répond aux besoins propres d'une entreprise en matière de sécurité et de performances à l'aide du kit de réalisation de logiciel SDK (*Software Development Kit*).
- Il étend les fonctionnalités de sécurité et de gestion avec des solutions d'autres fabricants.
- Il automatise les tâches administratives grâce aux objets COM (*Component Object Model*).

II.3 Les modes d'installation d'ISA server

➢ Mode cache

En mode cache, il peut améliorer les performances du réseau et économiser de la bande passante en stockant les objets Web auxquels les utilisateurs accèdent souvent. Il peut ensuite router les demandes des clients vers un serveur de cache qui contient les objets mis en cache.

➢ Mode pare-feu

En mode pare-feu, il peut sécuriser le trafic réseau en configurant des règles qui contrôlent la communication entre un réseau interne et Internet. Il peut également publier des serveurs internes, qui permettent à une entreprise de partager des données sur son réseau avec des partenaires ou clients.

➢ Mode intégré

En mode intégré, il peut associer les services de pare-feu et de cache sur un même ordinateur hôte. Même si les entreprises peuvent déployer ISA Server en tant que pare-feu ou serveur de cache distinct, rien n'empêche d'associer le serveur de pare-feu et le serveur de cache en choisissant le mode intégré. De nombreuses entreprises peuvent tirer parti d'une administration unifiée des fonctions de mise en cache et de pare-feu.

II.4 Fonctionnalités propres à chaque mode

En fonction du mode choisi, il dispose de différentes fonctionnalités. Le tableau II.1 répertorie les fonctionnalités disponibles pour les modes pare-feu et cache. En mode intégré, l'ensemble des fonctionnalités est disponible.

Fonctionnalité	**Description**	**Mode pare-feu**	**Mode cache**
Stratégie d'accès	Définit les protocoles et le contenu Internet auxquels accèdent des ordinateurs clients situés derrière un ordinateur exécutant ISA Server.	Oui	HTTP et FTP seulement
Mise en cache Web	Stocke les objets Web souvent récupérés dans la mémoire vive et sur le disque dur d'un ordinateur exécutant ISA Server	Non	Oui
Réseaux VPN	Étend un réseau privé en utilisant des liens entre des réseaux partagés ou publics, tels qu'Internet.	Oui	Non
Filtrage de paquets	Contrôle le flux de paquets IP à destination et en provenance de la carte externe d'un ordinateur exécutant ISA Server.	Oui	Non
Filtres d'application	Exécutent des tâches propres au protocole ou au système, telles que l'authentification, pour fournir une couche de sécurité supplémentaire au service de pare-feu.	Oui	Non
Publication Web	Met les serveurs Web internes à la disposition d'ordinateurs clients externes.	Non	Oui
Publication de serveurs	Met les serveurs d'application internes à la disposition des ordinateurs clients externes.	Oui	Non
Surveillance en temps réel	Permet de surveiller de manière centralisée l'activité d'un ordinateur exécutant ISA Server, notamment les alertes, les sessions et les services.	Oui	Oui
Alertes	Vous avertissent lorsque des événements particuliers se produisent et exécutent les actions appropriées.	Oui	Oui
Rapports	Résument et analysent l'activité qui se produit sur un ou plusieurs ordinateurs exécutant ISA Server.	Oui	Oui

Tableau II.1 : les fonctionnalités propres à chaque mode d'ISA server

II.5 Utilisation de la mise en cache

La mise en cache améliore les performances du réseau grâce à un cache contenant les objets Web auxquels les utilisateurs accèdent fréquemment.

II.5.1 Processus de mise en cache

Le processus utilisé par ISA Server pour mettre en cache du contenu est similaire à celui utilisé par un navigateur Web pour enregistrer les fichiers Internet temporaires. La plupart des navigateurs Web mettent en cache des objets localement, c'est-à-dire qu'ils stockent les pages Web demandées dans un dossier sur le disque dur de l'ordinateur. Le navigateur Web accède ensuite à ces mêmes objets en les récupérant sur le disque dur local. ISA Server pousse cette logique un peu plus loin puisqu'il gère un cache centralisé des objets Web les plus souvent demandés afin d'améliorer les performances pour plusieurs utilisateurs. Les étapes ci-dessous décrivent le processus de mise en cache utilisé par ISA Server pour récupérer des objets Web pour des ordinateurs clients.

1. L'ordinateur client 1 demande un objet Web.
2. Si cet objet n'est pas déjà dans le cache ISA Server, ISA Server le récupère sur Internet à partir du serveur Web.
3. Le serveur Web sur Internet renvoie l'objet à l'ordinateur exécutant ISA Server, qui conserve une copie de l'objet dans son cache et renvoie l'objet à l'ordinateur client 1. Le temps nécessaire au client pour recevoir l'objet et le trafic Internet qui en résulte sont approximativement les mêmes que si le client avait accédé directement à l'objet.
4. Le client 2 demande le même objet Web.
5. ISA Server renvoie l'objet qu'il a dans son cache au lieu de le récupérer sur Internet à partir du serveur Web. L'ordinateur client reçoit l'objet très rapidement et cette demande ne génère pas de trafic Internet.

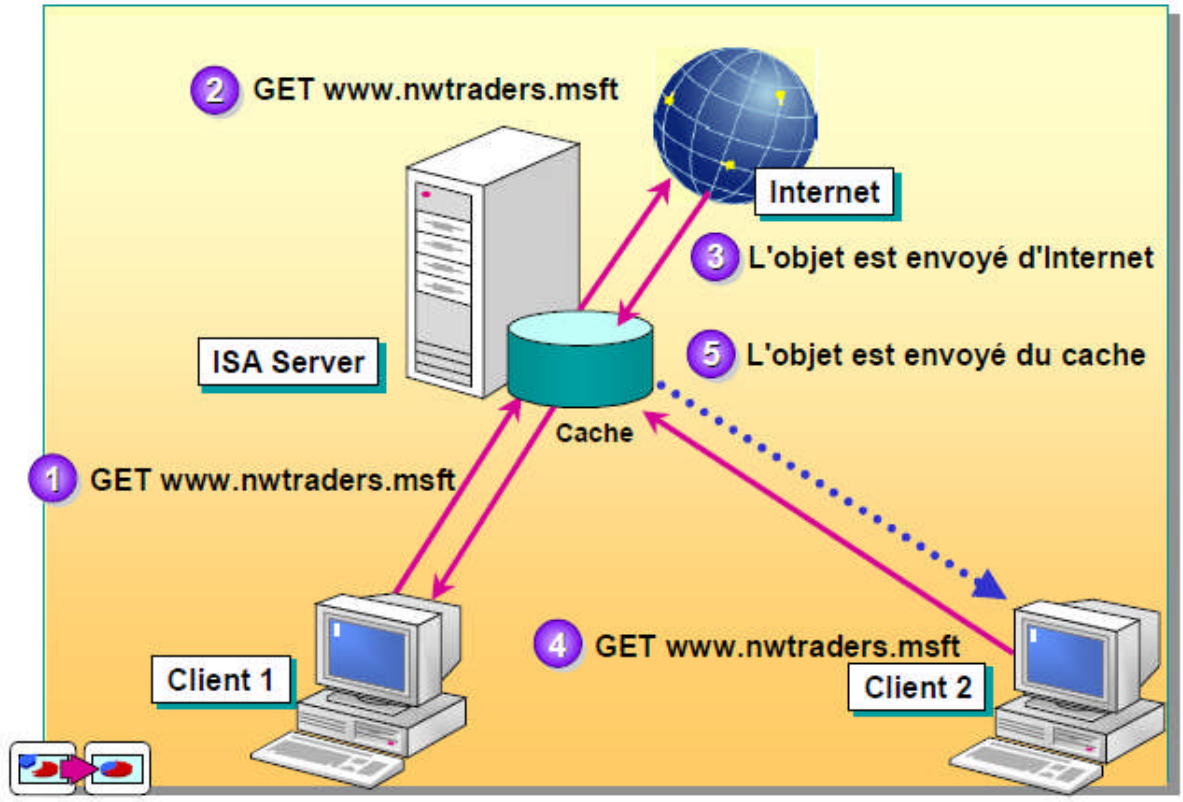


Figure II.1 : Processus de mise en cache

II.5.2 Types de mises en cache

Le service de mise en cache accélère les performances Web aussi bien pour les ordinateurs clients internes que pour les ordinateurs clients externes. ISA Server prend en charge la mise en cache directe pour les demandes sortantes, la mise en cache inversée pour les demandes entrantes et il peut être aussi distribué sur plusieurs ordinateurs exécutant ISA Server.

➢ Mise en cache directe

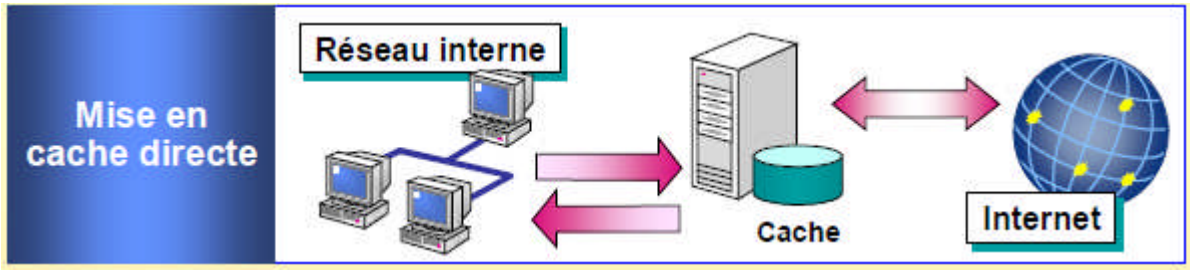


Figure II.2 : Mise en cache directe

La mise en cache directe (figure II.2) permet de fournir aux ordinateurs clients internes un accès aux objets Web sur Internet. L'ordinateur exécutant ISA Server gère un cache centralisé des objets Web les plus souvent demandés et qui sont accessibles à partir de tout navigateur Web. Les objets distribués à partir du cache nécessitent moins de traitement que ceux récupérés à partir d'Internet.

➢ Mise en cache inversée

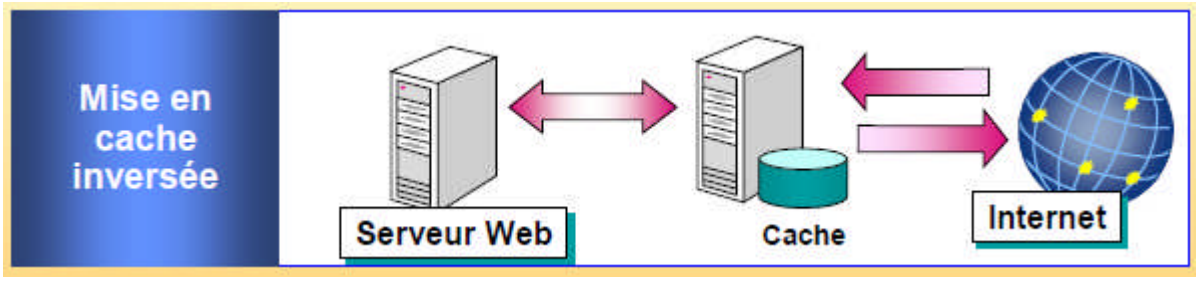


Figure II.3 : Mise en cache inversée

La mise en cache inversée (Figure II.3) permet de fournir aux ordinateurs clients externes un accès aux objets Web à partir d'un serveur Web interne. L'ordinateur exécutant ISA Server, qui est situé devant le serveur Web, transmet les demandes au serveur Web interne uniquement s'il ne peut pas récupérer un objet demandé dans son cache. ISA Server accélère la vitesse à laquelle les clients externes reçoivent les objets Web.

➢ Mise en cache distribuée

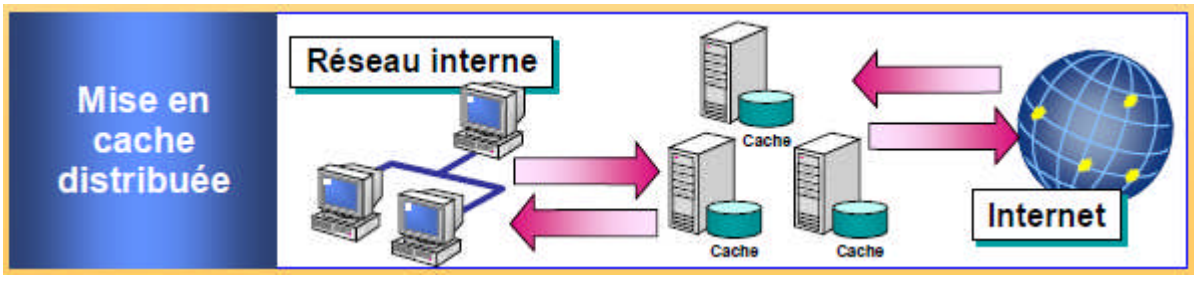


Figure II.4 : Mise en cache distribuée

On configure un groupe d'ordinateurs exécutant ISA Server afin de réaliser une mise en cache distribuée. Un groupe d'ordinateurs ISA Server se gère comme une seule entité logique. La distribution d'objets mis en cache améliore les performances de la mise en cache grâce à l'équilibrage de la charge, et garantit la tolérance de panne si un ordinateur exécutant ISA Server est indisponible. Il peut distribuer aussi bien la mise en cache directe que la mise en cache inversée.

II.6 Utilisation de pare-feu

Un pare-feu est un système constitué de logiciels, de composants matériels, ou d'une association des deux, conçu pour protéger les réseaux privés des accès non autorisés. Il existe plusieurs conceptions de pare-feu, notamment les hôtes bastions et les réseaux périphériques avec un pare-feu tri-résident ou avec des pare-feu dos-à-dos. Les pare-feu utilisent le filtrage de paquets et d'autres types de filtrage pour contrôler l'accès au réseau.

II.6.1 Vue d'ensemble des pare-feux

Le pare-feu permet de contrôler le trafic entrant et sortant. Il est installé à l'emplacement de l'interconnexion entre le réseau privé et Internet. Sur un réseau, un pare-feu empêche les éventuels dangers liés à Internet de se propager sur le réseau interne.
Les deux principales fonctions d'un pare-feu sont :

- Il s'agit d'un point d'accès sous contrôle pour tout le trafic qui entre sur le réseau interne.

Un pare-feu empêche des utilisateurs non autorisés d'accéder aux données et aux ressources de réseau.

- Il s'agit d'un point d'accès sous contrôle pour tout le trafic qui sort du réseau interne.

Un pare-feu permet de s'assurer que les interactions entre Internet et le réseau interne sont conformes aux règles et aux stratégies de sécurité de l'entreprise.

II.6.1.1 Hôte bastion

L'hôte bastion est l'ordinateur qui constitue le principal point de contact des clients des réseaux internes lorsqu'ils accèdent à Internet. En tant que pare-feu, l'hôte bastion est conçu pour défendre le réseau interne des attaques. Il est généralement utilisé sur les petits réseaux pour protéger le réseau interne des intrus.

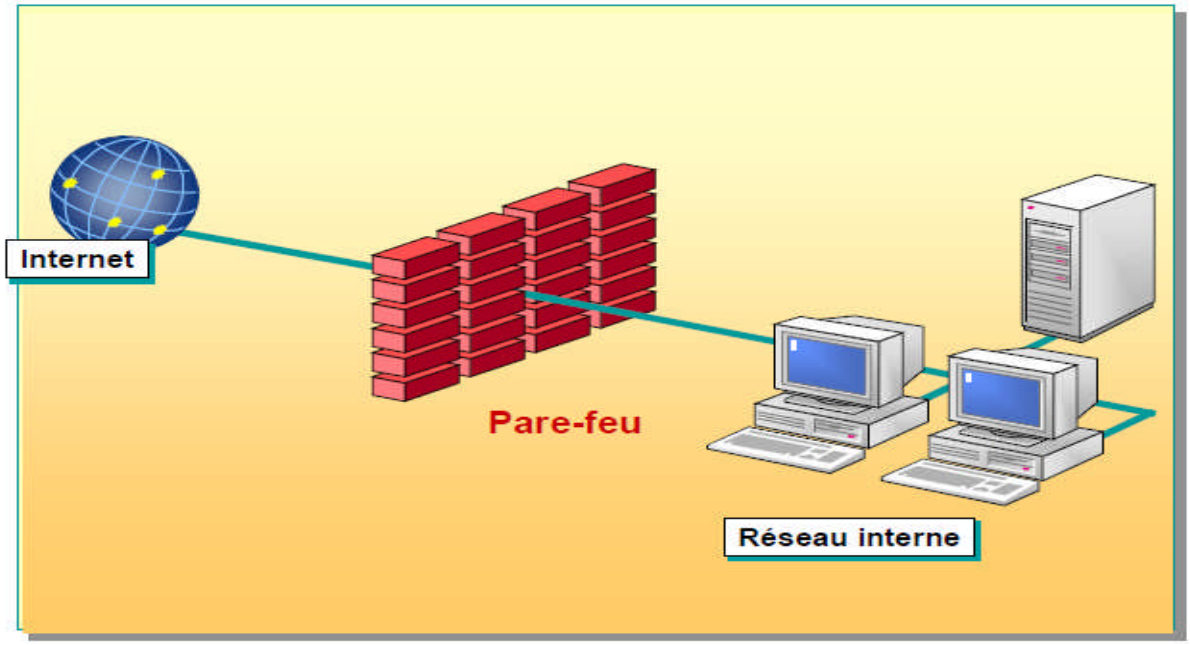


Figure II.5 : schéma d'un hôte bastion

➢ Configuration d'un hôte bastion

Un hôte bastion compte deux cartes réseau, l'une étant connectée au réseau interne et l'autre à Internet. Cette configuration isole physiquement le réseau interne des éventuels intrus se trouvant sur Internet. Puisque la configuration d'un hôte bastion ne consiste qu'en un seul point de défense, il est important de veiller à ce que l'ordinateur qui joue ce rôle soit correctement sécurisé.

➢ Avantage lié à l'utilisation d'un hôte bastion

Il permet de réduire le coût et le volume des tâches administratives requises pour un pare-feu. Cependant, un hôte bastion dépend d'un seul pare-feu pour protéger l'ensemble du réseau. Si un internaute compromet le pare-feu, il peut accéder au réseau interne de l'entreprise, notamment aux ressources qui ne sont pas suffisamment sécurisées.

Sachant qu'un hôte bastion permet aux internautes d'accéder directement au réseau interne, il faut recourir à d'autres moyens pour protéger les ressources internes, par exemple définir des autorisations d'accès strictes sur les ressources réseau.

II.6.1.2 Réseau périphérique équipé d'un pare-feu tri-résident

Un réseau périphérique est un petit réseau qui contient les ressources qui peuvent être mises à la disposition des internautes tout en assurant la sécurité de ces ressources. Un réseau périphérique est séparé de réseau interne et d'Internet. Un réseau périphérique permet aux clients externes d'accéder à des serveurs spécifiques situés sur le réseau périphérique tout en empêchant totalement l'accès au réseau interne. Un tel réseau sert généralement à déployer des serveurs Web ou des serveurs de messagerie. Un réseau périphérique peut être configuré de deux façons : avec un pare-feu tri-résident ou avec des pare-feu dos-à-dos.

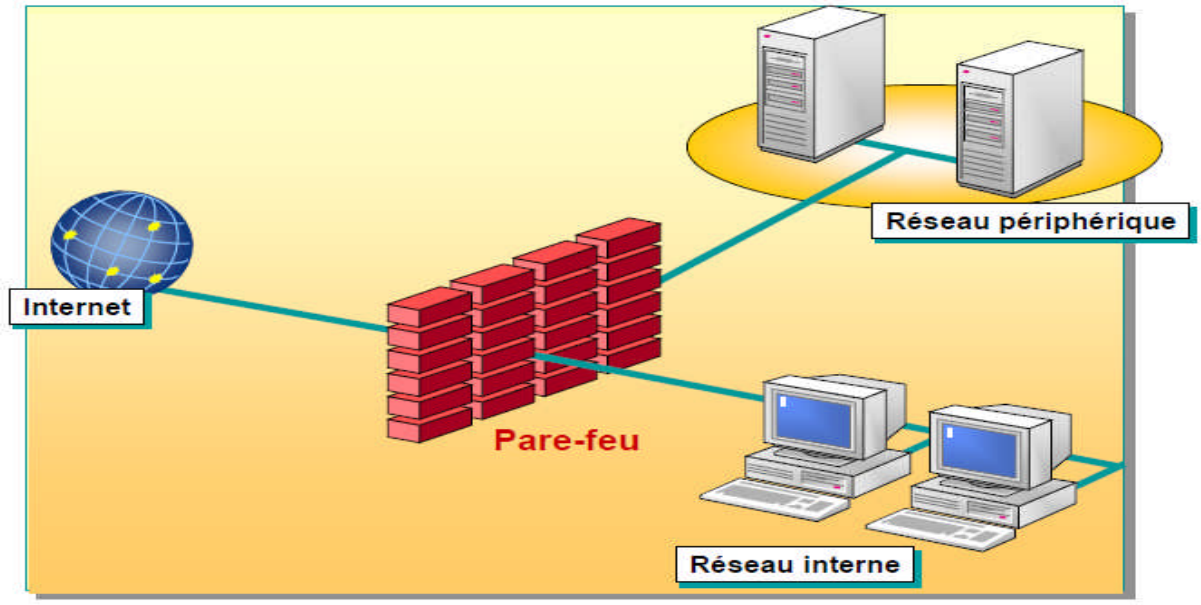


Figure II.6 : schéma d'un réseau équipé d'un pare-feu tri-résident

- **Configuration d'un réseau périphérique avec un pare-feu tri-résident**

S'il s'agit d'un réseau périphérique avec un pare-feu tri-résident, le pare-feu est configuré avec trois cartes réseau. Chaque carte réseau est connectée à l'un des réseaux suivants :

- Internet.
- Les serveurs du réseau interne situés sur le réseau périphérique.
- Les clients du réseau interne.

Bien que les serveurs du réseau périphérique aient chacun des adresses IP (*Internet Protocol*) auxquelles les clients externes peuvent accéder, l'ordinateur pare-feu ne permet pas d'accéder directement aux ressources qui sont situées sur le réseau interne.

La stratégie de sécurité d'une entreprise peut également autoriser un trafic réseau restreint et très contrôlé entre les ordinateurs du réseau périphérique et des ordinateurs sélectionnés sur le réseau interne.

- **Avantages liés à l'utilisation d'un réseau périphérique équipé d'un pare-feu tri-résident**

Un pare-feu tri-résident fournit une meilleure sécurité qu'un hôte bastion, car il permet un accès sécurisé à certaines ressources réseau à partir d'Internet sans autoriser le trafic réseau entre Internet et le réseau interne. Un pare-feu tri-résident fournit un seul point d'administration permettant de configurer l'accès à votre réseau périphérique et au réseau interne. Toutefois, un pare-feu tri-résident fournit aussi un seul point d'accès à toutes les parties de réseau, ce qui signifie qu'il doit être particulièrement attentif à la conception des règles d'accès et à la surveillance des violations de sécurité.

II.6.1.3 Réseau périphérique équipé de pare-feu dos-à-dos

Outre un réseau périphérique équipé d'un pare-feu tri-résident, on peut configurer un réseau périphérique avec des pare-feu dos-à-dos.

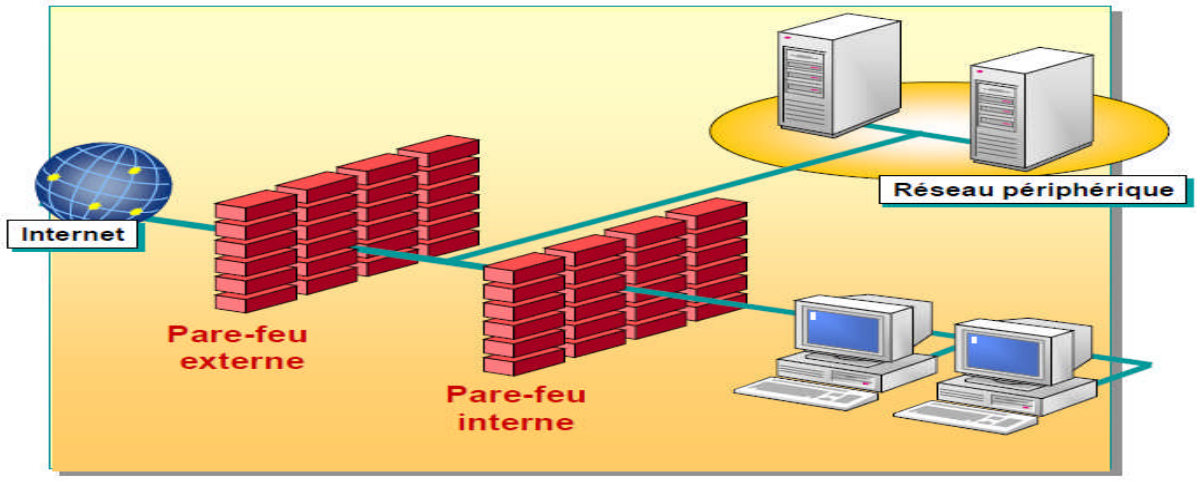


Figure II.7 : Schéma d'un réseau périphérique équipé de pare-feu dos-à-dos

- **Configuration des pare-feu dos-à-dos**

Sur un réseau périphérique équipé de pare-feu dos-à-dos, deux pare-feu sont situés de chaque côté du réseau périphérique. Ces deux pare-feu sont connectés au réseau périphérique, l'un étant également connecté à Internet et l'autre l'étant au réseau interne. Dans cette configuration, il n'y pas de point d'accès. Pour atteindre le réseau interne, un utilisateur doit en effet traverser les deux pare-feu.

- **Avantages liés à l'utilisation des pare-feu dos-à-dos**

On peut configurer des règles de sécurité plus strictes sur des pare-feu dos-à-dos que sur un pare-feu tri-résident, ce qui permet de protéger votre réseau interne de façon plus fiable.

Il est également plus facile de configurer des règles pour des pare-feu dos-à-dos si la stratégie d'accès de l'entreprise autorise un trafic réseau restreint et très contrôlé entre des ordinateurs du réseau périphérique et des ordinateurs sélectionnés sur le réseau interne.

II.6.2 Les filtres d'ISA Server

ISA Server permet de contrôler l'accès au réseau à la fois pour le trafic entrant et pour le trafic sortant. Pour contrôler le trafic sortant, on peut utiliser des règles et des stratégies d'accès. Pour contrôler le trafic entrant, on peut utiliser des filtres de paquets IP, des filtres d'application et des filtres de détection d'intrusion.

II.6.2.1 Contrôle du trafic sortant

Les règles et stratégies d'accès permettent de contrôler le trafic sortant. Une stratégie d'accès est constituée des règles énoncées ci-dessous.

- Règles sur les protocoles : Définissent les protocoles auxquels les utilisateurs peuvent recourir pour les communications établies entre le réseau interne et Internet. Par exemple, une règle sur les protocoles peut autoriser les clients à utiliser le protocole HTTP (HyperText Transfer Protocol).
- Règles sur les sites et le contenu : Définissent le contenu et les sites Internet auxquels les utilisateurs peuvent accéder. Par exemple, une règle sur les sites et le contenu peut autoriser les utilisateurs à accéder à tout site Internet.

ISA Server masque également les adresses IP sur le réseau interne lorsque des clients sont connectés à Internet. Les utilisateurs externes ont ainsi plus de difficultés à découvrir la structure de réseau interne et donc à y accéder.

II.6.2.2 Contrôle du trafic entrant

Les filtres de paquets IP, les filtres circuits et les filtres d'application permettent de contrôler le trafic entrant.

- **Filtres de paquets IP**

Les filtres de paquets IP fonctionnent dans les couches réseau et transport de modèle OSI, ils permettent de contrôler l'accès au réseau en fonction des caractéristiques des paquets réseau. Le ISA Server intercepte évalue les paquets avant de les faire passer au niveau supérieur, les filtres de paquets IP analysent les en-têtes de chaque paquet IP.
Par défaut en appliquant les filtres au niveau paquets, ISA interdit tous les paquets destinés au réseau interne provenant du réseau externe. Le filtre paquet permet d'ouvrir les ports de manière statique. Deux types de filtres peuvent être définis : autoriser et/ou bloquer. La politique d'accès et les règles de publication ouvre les ports de façon dynamique, c-à-dire que le port est fermé tant qu'une requête d'ouverture n'est pas arrivée.
ISA Server permet d'autoriser ou de refuser les paquets réseau en fonction des caractéristiques d'un paquet IP, notamment :

- L'adresse source ou de destination.
- Le protocole réseau, par exemple ICMP (*Internet Control Message Protocol*) ;
- Le numéro de port TCP ou UDP.

- **Filtres de circuit**

Le filtrage circuit est établi au niveau transport. Quand un filtre circuit est utilisé, le contrôle d'accès est basé sur les trames TCP ou les datagrammes UDP. Le filtrage au niveau circuit permet d'inspecter les sessions plutôt que les paquets. Une session est souvent vue comme une connexion, mais une session peut contenir plusieurs connexions. Les sessions ne sont établies qu'en réponse à une demande utilisateur, ce qui rajoute à la sécurité.

- **Filtres d'application**

Les filtres d'application fonctionnent sur la dernière couche de modèle OSI, ils acceptent ou refusent les données provenant de certaines applications ou les données ayant un contenu particulier. Ils examinent le trafic réseau qui s'étend sur plusieurs paquets IP, par exemple un message électronique complet. ISA Server comprend plusieurs filtres d'application qui sont automatiquement installés avec ISA Server, notamment ceux indiqués ci-dessous.

- Filtre de diffusion multimédia par flux : Il permet de contrôler l'accès aux données des clients utilisant des protocoles de diffusion multimédia par flux pour accéder aux serveurs de diffusion multimédia par flux, comme Microsoft Windows Media Technology (WMT) Server.

- Filtre SMTP *(Simple Mail Transfer Protocol)* : Il filtre le courrier électronique entrant en fonction de sa source, de l'utilisateur ou du domaine, puis génère l'alerte correspondante. Le filtre tient à jour la liste des utilisateurs et des domaines refusés, c'est-à-dire des quels les messages électroniques ne sont pas acceptés.

De nombreux experts firewall considèrent que les filtres application sont les plus sécurisés des technologies de filtrage, car les critères sont plus larges que les autres méthodes.

- **Filtres de détection d'intrusion**

ISA Server comprend plusieurs filtres de détection d'intrusion, notamment ceux indiqués ci-dessous.

- Filtre de détection d'intrusion DNS : Il intercepte et analyse le trafic DNS (Domain Name System) destiné au réseau interne. Ce filtre traque les diverses attaques connues contre les serveurs DNS et les empêche d'atteindre ces serveurs.

- Filtre de détection d'intrusion POP : Il intercepte et analyse le trafic POP (Post Office Protocol) destiné au réseau interne et empêche les attaques d'atteindre le serveur POP.

II.6.2.3 Processus de filtrage

Le filtrage des données dans le ISA server prend le chemin suivant :

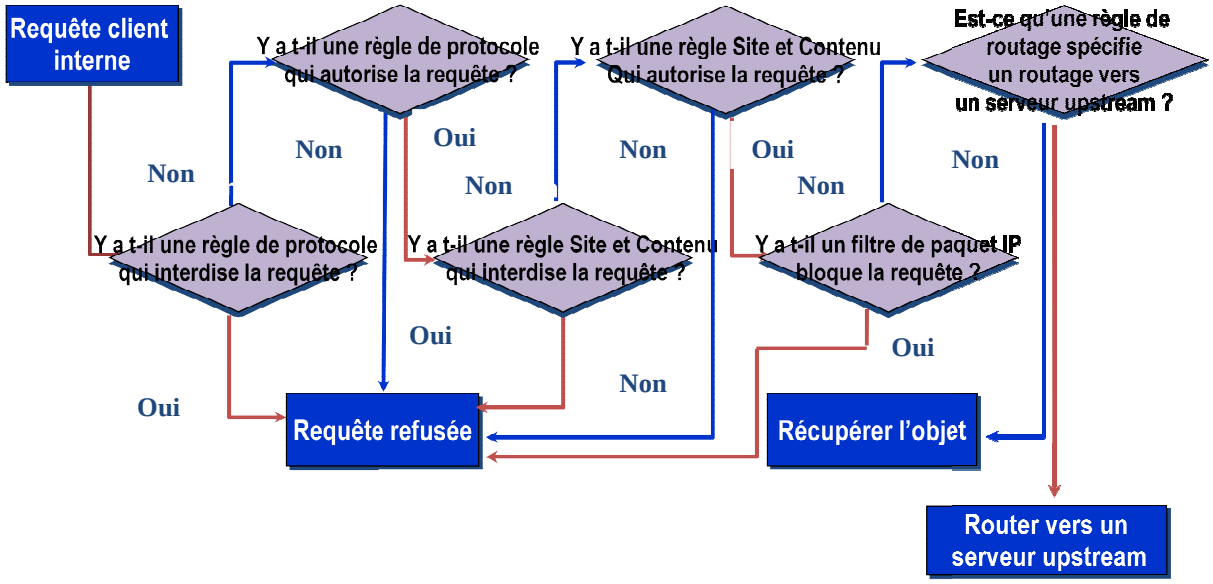


Figure II.8 : Le processus du filtrage

II.7 Les clients d'ISA serveur

Client proxy Web : il se configure dans les propriétés. L'accès à Internet est par conséquent limité au navigateur (et aux applications capables de récupérer les paramètres du navigateur). Son utilisation améliore les performances des requêtes Web.

Client Secure NAT : la configuration d'un client Secure NAT se fait en déclarant comme passerelle du client l'adresse IP du serveur ISA. Ce type permet de bénéficier de la sécurité et de la mise en cache, mais n'offre pas de mécanisme d'authentification au niveau de l'utilisateur.

Client pare-feu : c'est le seul à nécessiter l'installation d'un logiciel client. Il permet la limitation des demandes sortantes utilisant TCP et UDP par utilisateur. L'installation peut se faire depuis un partage créé à l'installation d'ISA ou à partir d'une interface web.

II.8 L'authentification par le ISA server

ISA Server 2006 permet de configurer différentes méthodes d'authentification basées sur les formulaires, les mots de passe et les protocoles pour les applications prises en charge.

➢ Authentification unique (SSO)

L'authentification unique permet aux utilisateurs de s'authentifier une seule fois sur Microsoft ISA Server et d'avoir accès à tous les serveurs Web dotés du même suffixe de domaine que Microsoft ISA Server publie sur un port d'écoute spécifique, sans procéder à une nouvelle authentification. Les serveurs Web peuvent être des serveurs Microsoft Outlook Web Access et des serveurs exécutant Microsoft Office SharePoint Portal Server 2003.

➢ Authentification à deux facteurs

L'authentification à deux facteurs garantit une sécurité renforcée car l'utilisateur doit respecter deux critères d'authentification : une combinaison nom d'utilisateur/mot de passe et un jeton ou certificat. ISA Server gère l'authentification à deux facteurs dans les scénarios suivants :

- L'utilisateur possède un certificat.
- L'utilisateur possède un jeton SecurID qui fournit un code.
- L'utilisateur possède un jeton contenant un mot de passe à usage unique qui fournit un code.

➢ Authentification par formulaires

L'authentification par formulaires dans ISA Server 2006 peut être utilisée pour la publication d'un serveur Web. Il existe trois types d'authentification par formulaires dans ISA Server :

- **Formulaire avec mot de passe :** L'utilisateur entre un nom d'utilisateur et un mot de passe sur le formulaire. Il s'agit du type d'informations requises pour la validation des informations d'identification Active Directory, LDAP et RADIUS.
- **Formulaire avec code :** L'utilisateur entre un nom d'utilisateur et un code sur le formulaire. Il s'agit du type d'informations requises pour la validation des mots de passe à usage unique SecurID et RADIUS.
- **Formulaire avec mot de passe/code :** L'utilisateur entre un nom d'utilisateur et un code, ainsi qu'un nom d'utilisateur et un mot de passe. Le nom d'utilisateur et le code sont utilisés pour l'authentification auprès d'ISA Server avec les méthodes d'authentification par mot de passe à usage unique SecurID ou RADIUS, et le nom d'utilisateur et le mot de passe sont utilisés pour la délégation.

➢ Authentification HTTP

Il existe trois types d'authentification HTTP suivants :

- Authentification de base.
- Authentification Digest et WDigest.
- Authentification Windows intégrée.

- **Authentification de base**

La méthode d'authentification de base est une méthode standard largement utilisée qui permet de recueillir le mot de passe et le nom d'utilisateur. Cette authentification envoie et reçoit des informations utilisateur sous forme de caractères de texte pouvant être lus. Bien que les mots de passe et les noms d'utilisateurs soient codés, aucun cryptage n'est utilisé lors de l'authentification de base.

- **Authentification Digest et WDigest**

L'authentification HTTP inclut l'authentification Digest et l'authentification WDigest, qui est une nouvelle version de l'authentification Digest.

Authentification Digest : L'authentification Digest offre les mêmes fonctionnalités que l'authentification de base, mais la méthode de transmission des informations d'authentification est différente.

Authentification WDigest : Contrairement à l'authentification Digest traditionnelle, cette authentification n'impose pas que les mots de passe soient stockés en utilisant un chiffrement réversible. L'authentification WDigest, qui est gérée par ISA Server 2006, est une nouvelle version de l'authentification Digest dont les utilisateurs doivent taper leur nom d'utilisateur (et leur nom de domaine) exactement tel qu'il est stocké dans Active Directory.

- **Authentification Windows intégrée**

L'authentification Windows intégrée utilise les mécanismes d'authentification NTLM, Kerberos et Negotiate. Il s'agit de formes d'authentification sécurisées car le nom d'utilisateur et le mot de passe sont hachés avant d'être transmis sur le réseau. Lorsque l'authentification NTLM, Kerberos ou Negotiate sont activés, le navigateur de l'utilisateur reconnaît le mot de

passe grâce à un échange cryptographique avec le serveur Web, qui prend en compte le hachage des données.

- **Authentification des certificats de client**

Dans le scénario des certificats de clients, un certificat est fourni par le client, et ce dernier est authentifié par Microsoft ISA Server en fonction de ce certificat. Il peut s'agir d'un certificat intégré à une carte à puce ou d'un certificat utilisé par un périphérique portable pour une connexion à Microsoft.

II.9 La publication par le ISA server

La messagerie est un organe vital au bon fonctionnement d'une entreprise. Pour cela Microsoft avec l'outil ISA Server répond aux besoins rencontrés par les entreprises qui utilisent et publient le serveur de messagerie Exchange en toute sécurité.

La publication de messagerie Exchange par l'intermédiaire ISA Server permet d'empêcher un accès externe direct à votre serveur. Le nom et l'adresse IP du serveur Exchange ne sont pas divulgués à l'utilisateur. L'utilisateur se connecte, donc, au serveur ISA qui se charge de l'authentification du client en fonction de la stratégie mise en place. Si l'authentification est concluante, ISA crée le lien entre ce client et le serveur.

II.10 Utilisation des VPN

Le ISA Server 2006 inclut des fonctionnalités VPN intégrées, basées sur le service de routage et d'accès distant (RRAS) de Windows Server 2003. Il peut affecter des adresses IP à des clients VPN se connectant au réseau et peut appliquer une stratégie à tout le trafic distant.

Le ISA Server 2006 permet de configurer des clients VPN comme un réseau séparé et de créer des stratégies d'accès distinctes pour chaque client VPN. Le moteur de règles utilise la stratégie d'accès pour contrôler les requêtes des clients VPN, inspecter ces requêtes avec état et ouvrir dynamiquement des connexions entre les clients VPN et le réseau.

II.11 Conclusion

Avec Internet, de nouvelles opportunités s'offrent aux entreprises pour se connecter à leurs clients, leurs partenaires et leurs employés. Toutefois, Internet s'accompagne de nouveaux risques et de nouvelles préoccupations portant sur la sécurité, les performances et l'amélioration de la gestion. ISA Server est conçu pour répondre aux besoins actuels des entreprises présentes sur Internet. ISA Server apporte un pare-feu d'entreprise multicouche qui permet de protéger les ressources réseau contre les virus, les pirates informatiques et les accès frauduleux. Le cache Web d'ISA Server assure aux entreprises des économies de bande passante sur le réseau et accélère la connexion des utilisateurs au Web en prenant en charge les objets localement plutôt que par l'intermédiaire d'un réseau Internet saturé.

Chapitre III

La mise en œuvre d'une infrastructure réseau sécurisée par le ISA Server

Chapitre III : Mise en œuvre d'une infrastructure réseau sécurisée par le ISA Server

III.1 Introduction :

L'objectif de cette partie est de mettre en œuvre une infrastructure réseau sécurisée par le ISA Server, ce dernier permet aux clients de l'entreprise de partager des informations et des données en toute sécurité afin d'améliorer sa réactivité, sa compétitivité et ainsi devenir une « entreprise connectée ».

III.2 Cahier de charge

Pour la réalisation de notre travail, on dispose des paramètres suivants :

- VMware.
- 2 contrôleurs de domaine Active Directory (Microsoft Windows Server 2003).
- 1 serveur de messagerie (Exchange Server 2003).

III.3 Mise en place d'un réseau d'entreprise

Un réseau informatique est indispensable à toute organisation car il facilite la transmission, la duplication, le partage des dossiers et des périphériques. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données.

Il y a plusieurs façons de mettre en place un réseau d'entreprises (LAN), selon son architecture (client/serveur, client/client), sa topologie (bus, étoile, anneau,….) et selon les besoins.

Dans notre projet, nous avons opté pour une architecture (client/serveur). La figure suivante montre l'architecture du réseau avant de le sécuriser :

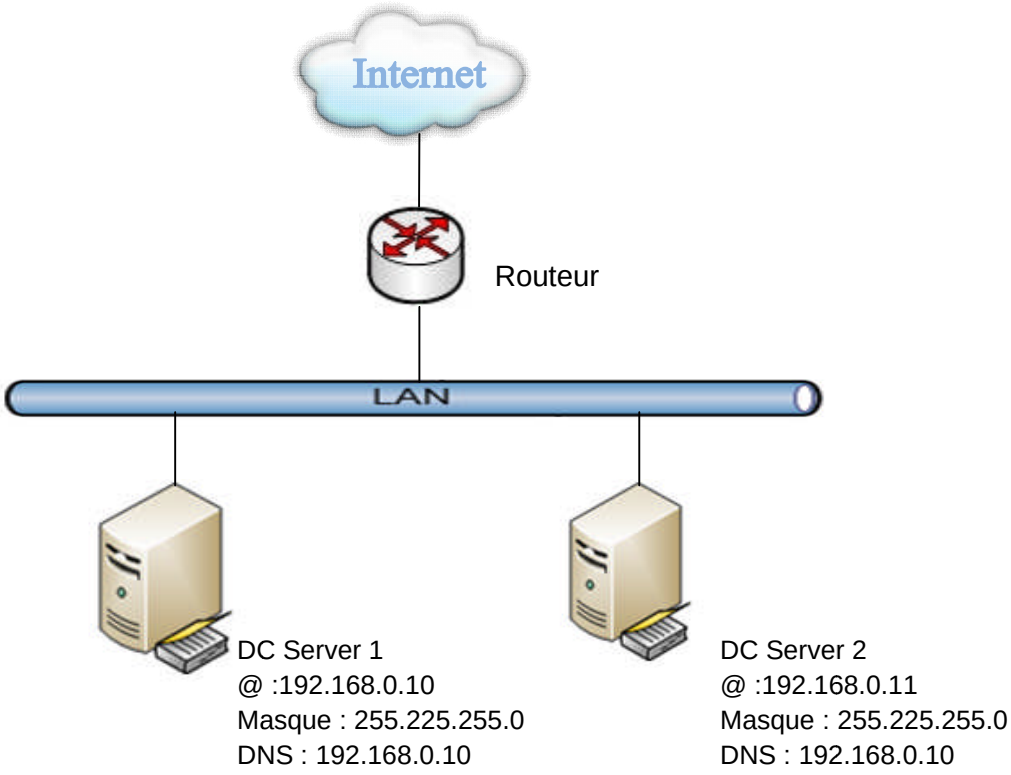


Figure III.1: Etat du réseau sans module de sécurité

III.4 Les problèmes liés à cette architecture

Cette architecture possède plusieurs problèmes dont on cite :

.Absence de sécurité.

. Augmentation rapide du nombre des utilisateurs.

· Volume accru du trafic généré par chaque utilisateur.

· Echange volumineux de fichiers non nécessaire entre utilisateurs.

· Augmentation accrue des bases de données.

· Trafic web important.

· Flux messagerie important.

III.5 La solution proposée :

Ajouter de nouveaux matériels qui doivent être utilisés par l'entreprise dans le but d'assurer le fonctionnement optimal de ses ressources réseaux et assurer à ses membres un accès rapide à l'information et un partage facile des données.

Pour cela on installe le serveur de sécurité ISA Server 2006 entre le réseau interne et le réseau externe (internet) qui joue le rôle d'un pare-feu logiciel qui protège le réseau local (LAN) contre les menaces internes et externes en provenance d'Internet

Et comme la messagerie est un élément vital au bon fonctionnement des entreprises, on utilise la fonctionnalité d'ISA Server pour publier le serveur de messagerie exchange 2003 en toute sécurité.

III.6 La mise en place de la solution

La figure ci-dessous représente le réseau après avoir ajouté un pare-feu et un serveur de messagerie :

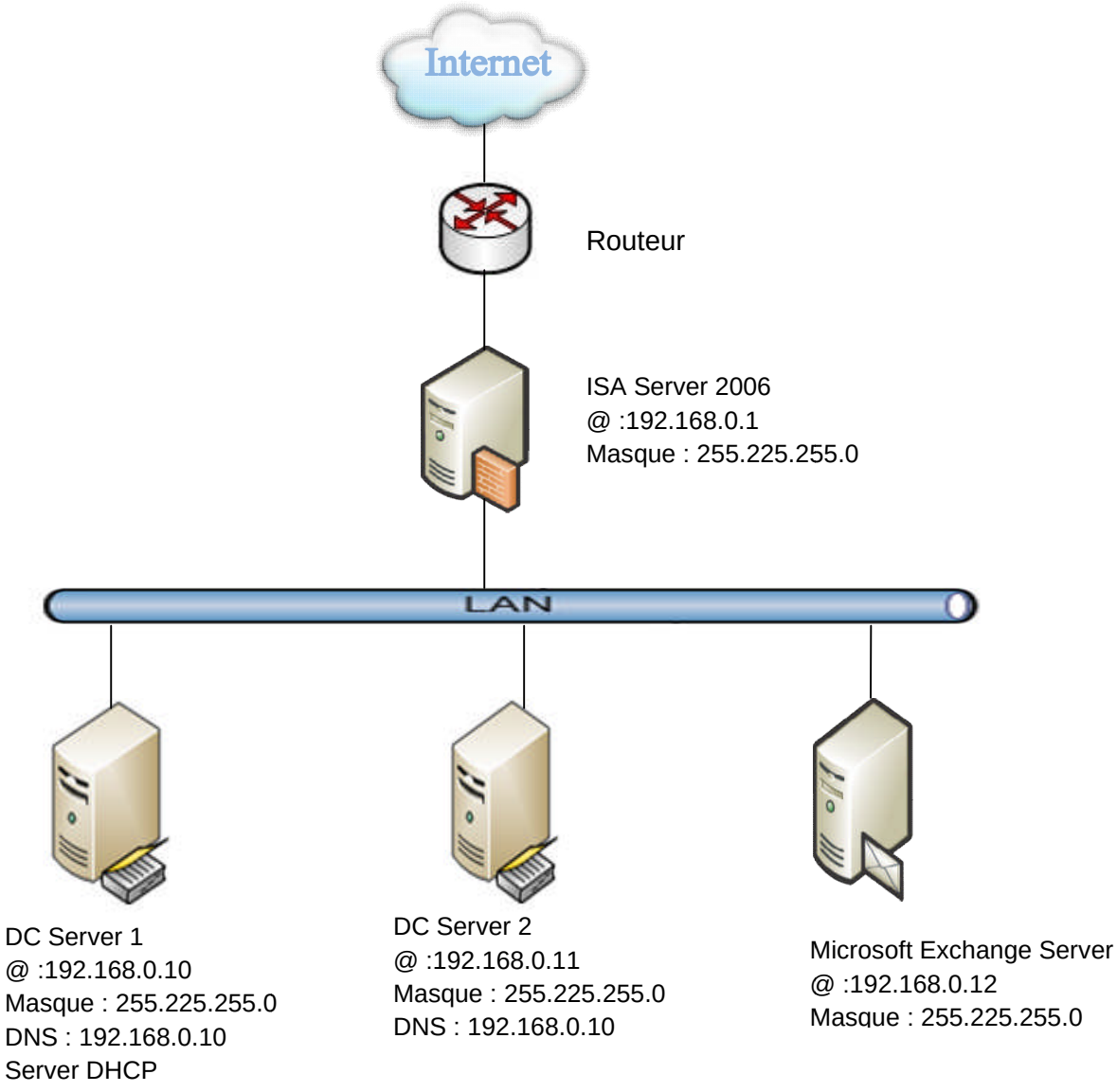


Figure III.2: Etat du réseau après l'intervention.

Pour réaliser cette architecture on crée des machines virtuelles avec le système d'exploitation Microsoft Windows 2003 server à l'aide du logiciel de virtualisation VMware.

- La première et la deuxième machine : on installe le service d'annuaire Active Directory et cela dans le but de créer deux contrôleurs de domaine le principal et le secondaire.
- La troisième machine : on installe Exchange Server 2003 pour la messagerie.
- La quatrième machine : on installe le ISA Server 2006 pour sécuriser tout le réseau.

III.7 Installations et configurations

III.7.1 Exigences matérielles et logicielles pour installer le ISA Server 2006

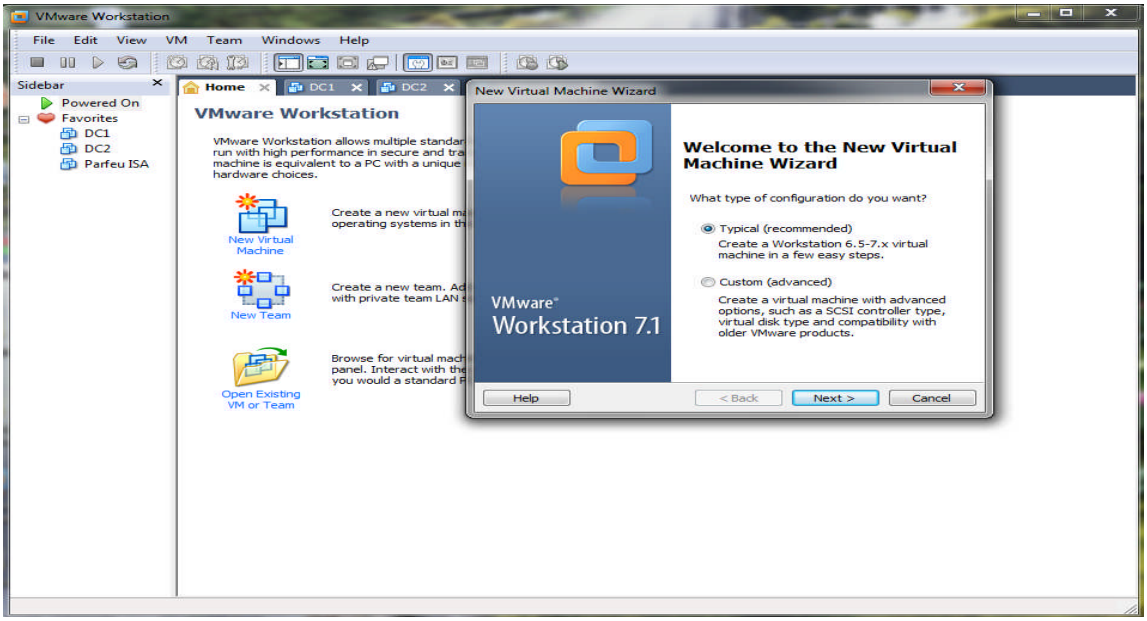
La configuration nécessaire à l'installation d'ISA dépend du nombre de machines connectées en même temps et des services utilisés. Il nécessite un environnement comportant les caractéristiques minimales suivantes :

Composant	Configuration requise
Système d'exploitation	Microsoft Windows Server 2003 avec Service Pack 1 (SP1) ou Microsoft Windows Server 2003 R2.
Processeur	PC équipé d'un Pentium III à 550 Mhz ou supérieur.
Mémoire vive	Au moins 512 Mo recommandée.
Disque dur	Partition locale formatée NTFS avec 150 Mo d'espace libre sur disque dur ; espace supplémentaire requis pour le contenu Web mis en cache.
Carte réseau	Deux cartes réseaux ou plus pour les fonctionnalités liées au pare-feu Une seule carte réseau si ISA est uniquement utilisé en tant que serveur de proxy

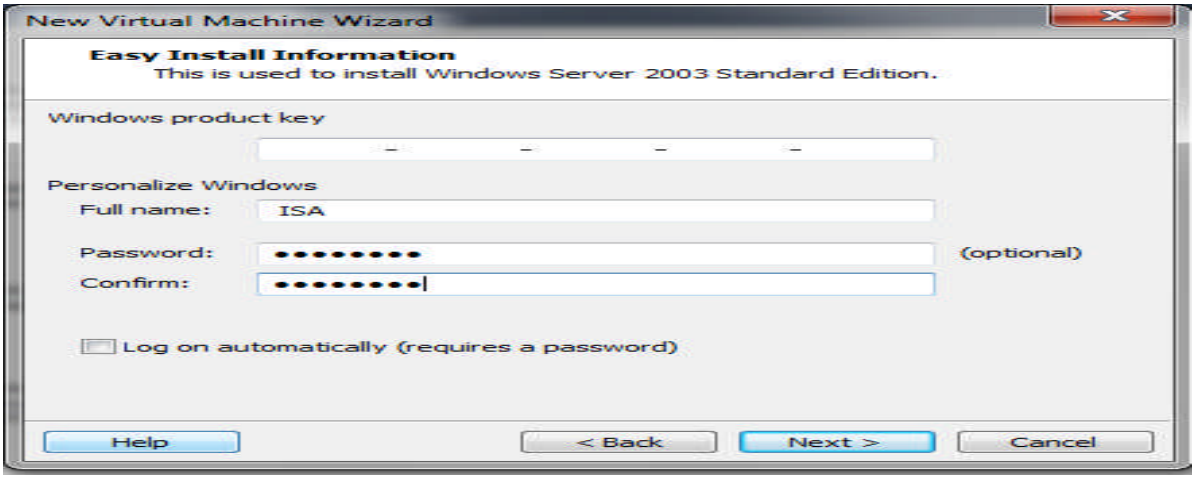
Tableau III.1: Configuration minimale requise pour l'installation d'ISA Server 2006.

III.7.2 Préparation de la machine

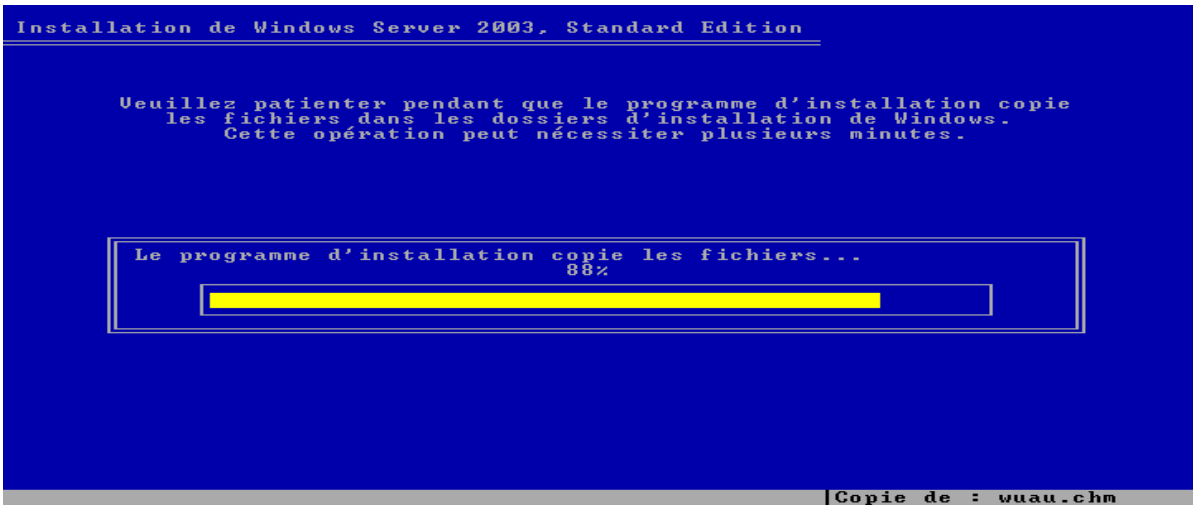
Créer une machine virtuelle avec VMware, pour ce faire on clique sur New virtuel Machine, une fenêtre s'ouvre et on clique sur Typical puis suivant :



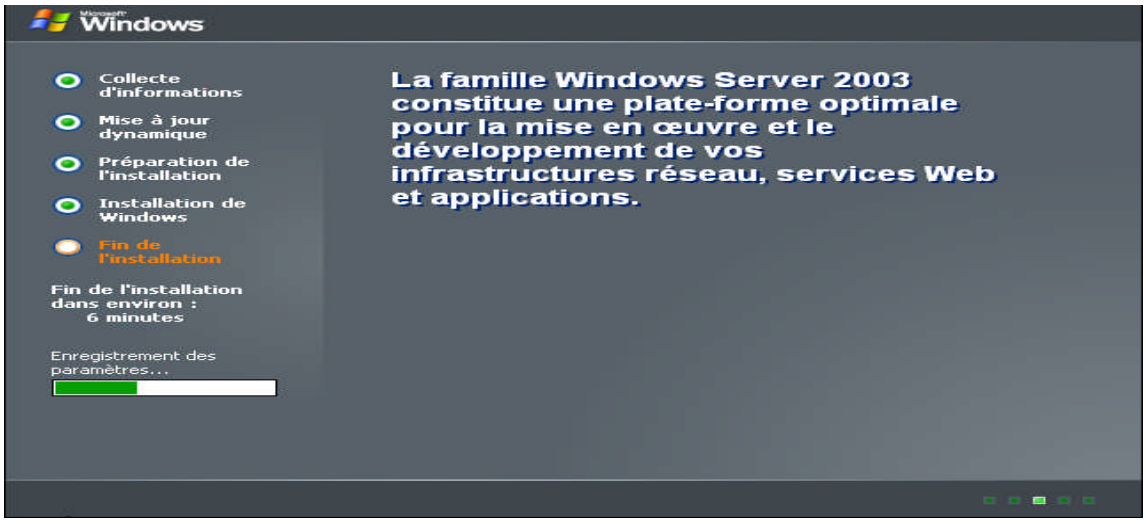
On insert le CD d'installation de Windows 2003 server et on choisit par disc, une fenêtre s'ouvre, on introduit la clé du produit, le nom de la machine (ISA) et le mot de passe puis on clique sur Next



Booter celle-ci avec le CD ROM de Windows Server 2003 que nous avons gravé



Le scénario d'installation va prendre un peu de temps pour copier les fichiers dans les dossiers d'installation de Windows 2003 Server.



Apres l'installation de Windows 2003 Server, on configure les adresses IP. La différence entre cette machine et les autres machines est que cette machine a deux interfaces réseaux; une connectée au réseau externe (internet) et la seconde connectée au réseau interne.

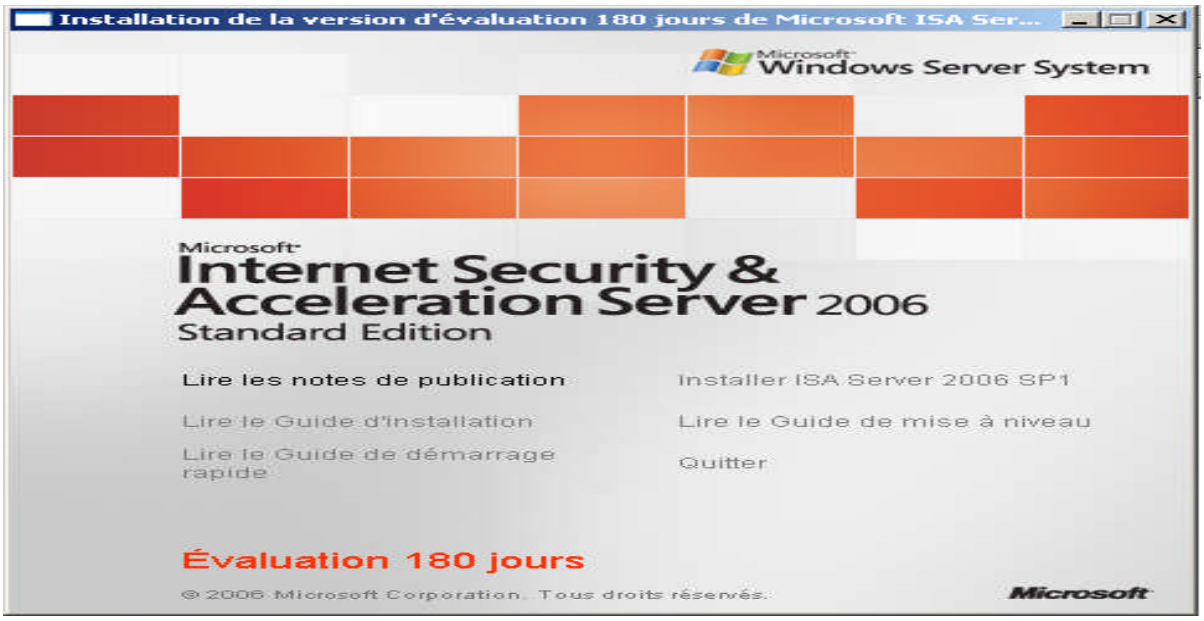
Avant de lancer l'installation d'ISA, on vérifie d'abord que la machine est bien intégrée dans le domaine Active Directory (2int.com).

Pour voir les paramètres réseaux de cette machine on tape la commande **ipconfig /all** dans la fenêtre invite de commande :

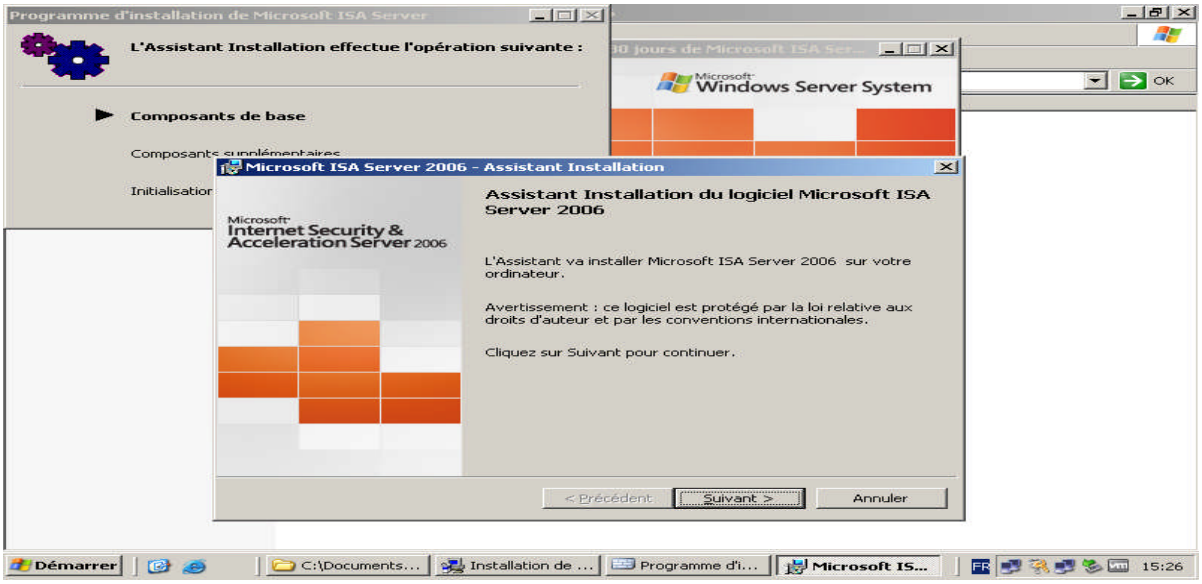
En termes de DNS, ce serveur ne pointe que sur les DNS d'Active Directory.

III.7.3 Installation du ISA Server 2006

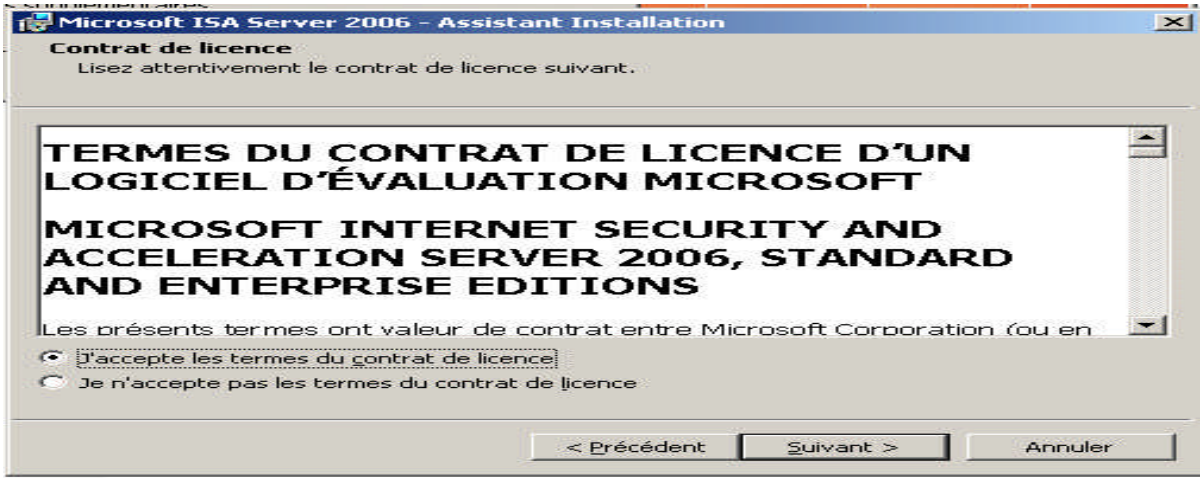
Apres avoir vérifié tous les paramétrages réseaux on lance l'installation de ISA, On double clique sur notre produit ISA Server 2006, une fenêtre s'ouvre :



Cliquer sur Installer ISA Server 2006 SP1, l'assistant d'installation se lance et on clique sur suivant pour continuer l'installation

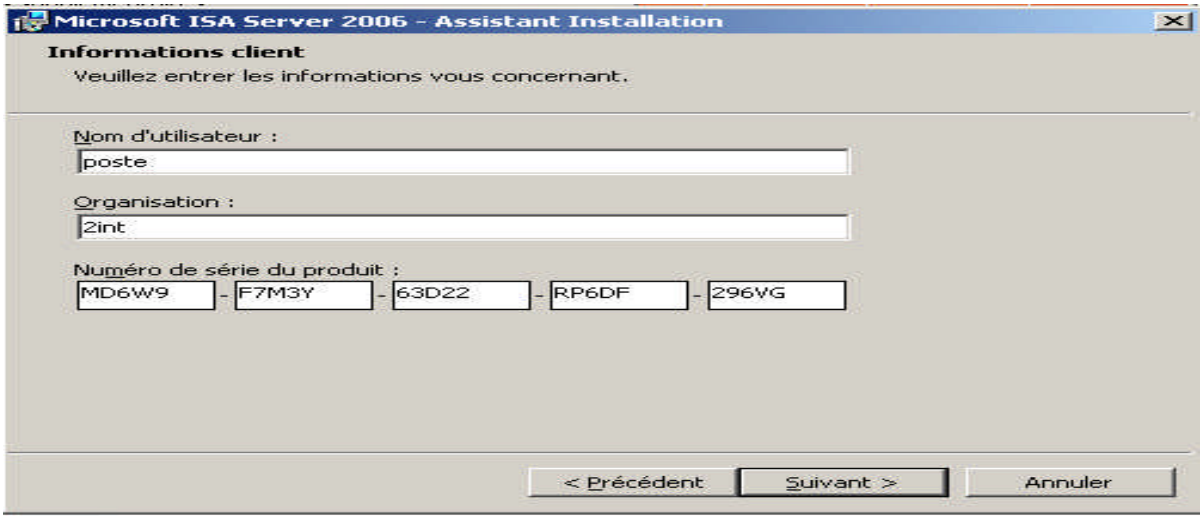


Une nouvelle fenêtre s'ouvre, c'est le contrat de licence de notre produit

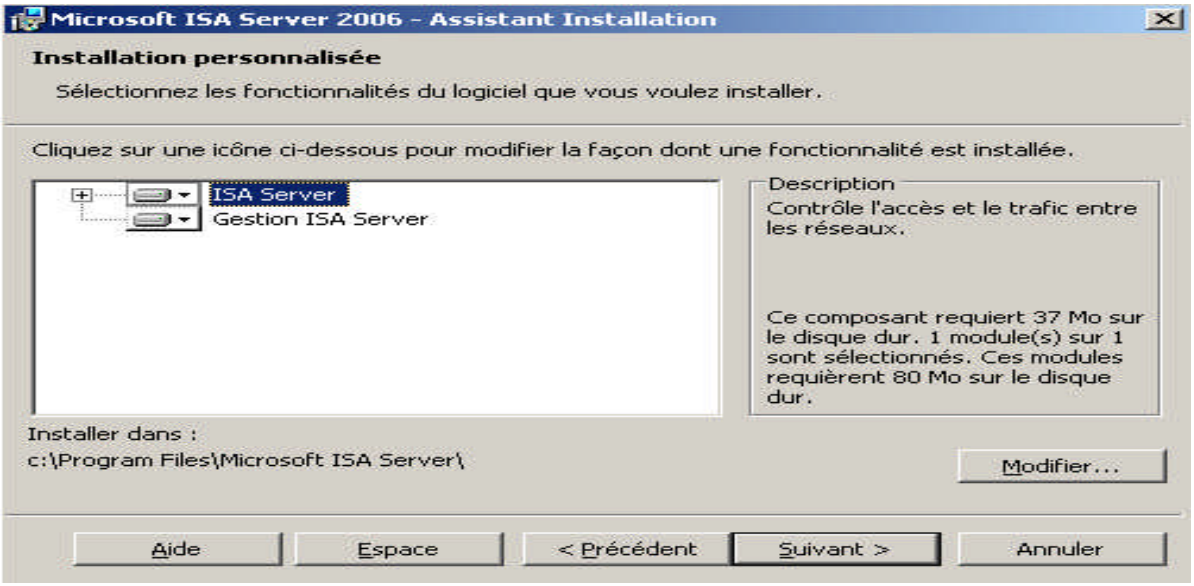


Apres avoir lu le contrat de la licence on coche « j'accepte les termes du contrat de licence » puis on clique sur suivant.

Une fenêtre s'ouvre dont on introduit la clé du produit, le nom d'utilisateur et l'organisation

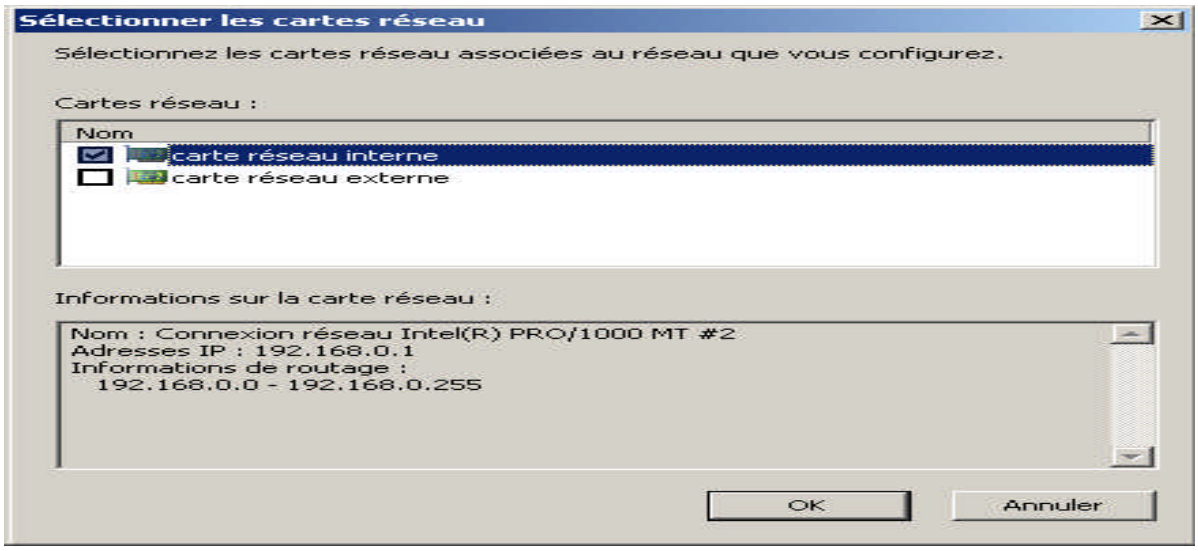


On clique sur suivant pour continuer, et sélectionner les fonctionnalités du ISA

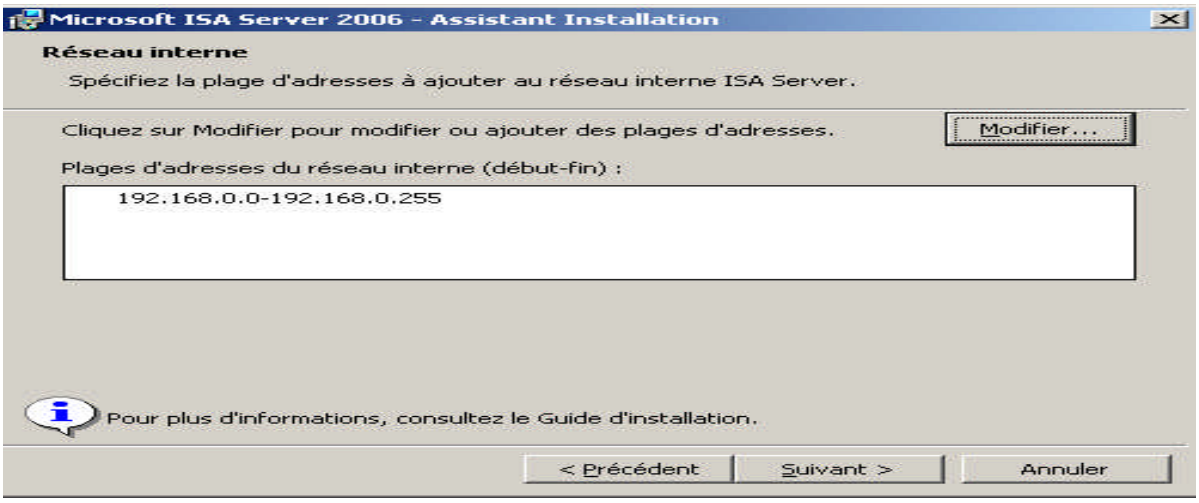


On clique sur suivant, une nouvelle fenêtre s'ouvre où on sélectionne les plages d'adresse du réseau interne.

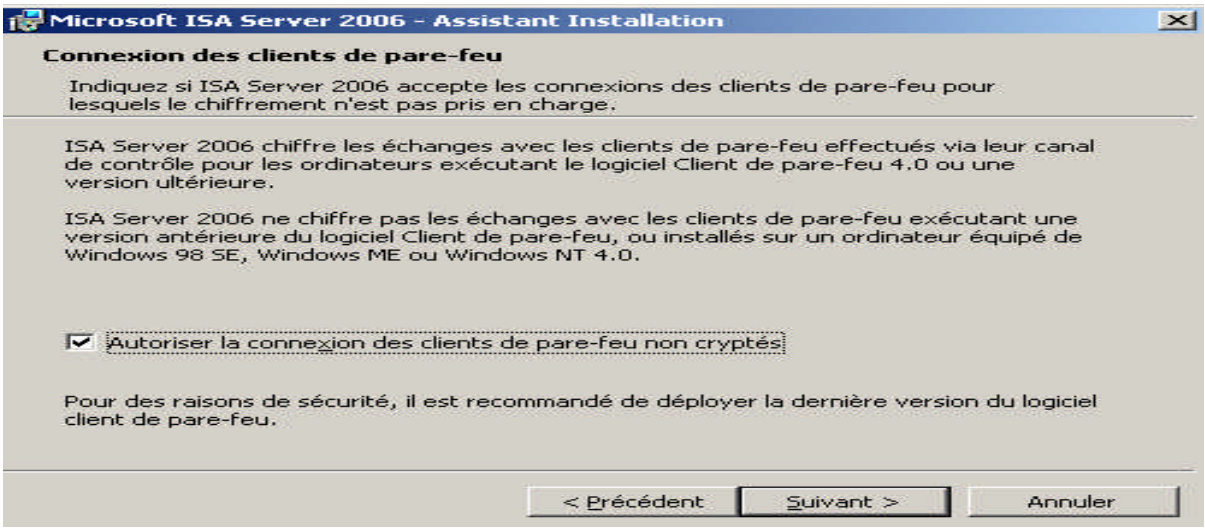
Pour définir cette plage, on clique sur Ajouter une carte réseau et cocher l'icône carte réseau interne puis on clique sur ok



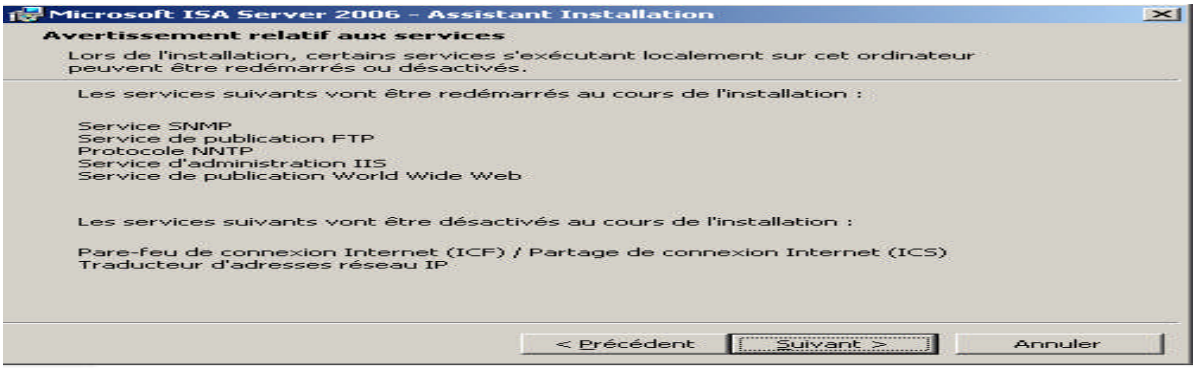
La plage du réseau interne est conçue par rapport à la table de routage Windows



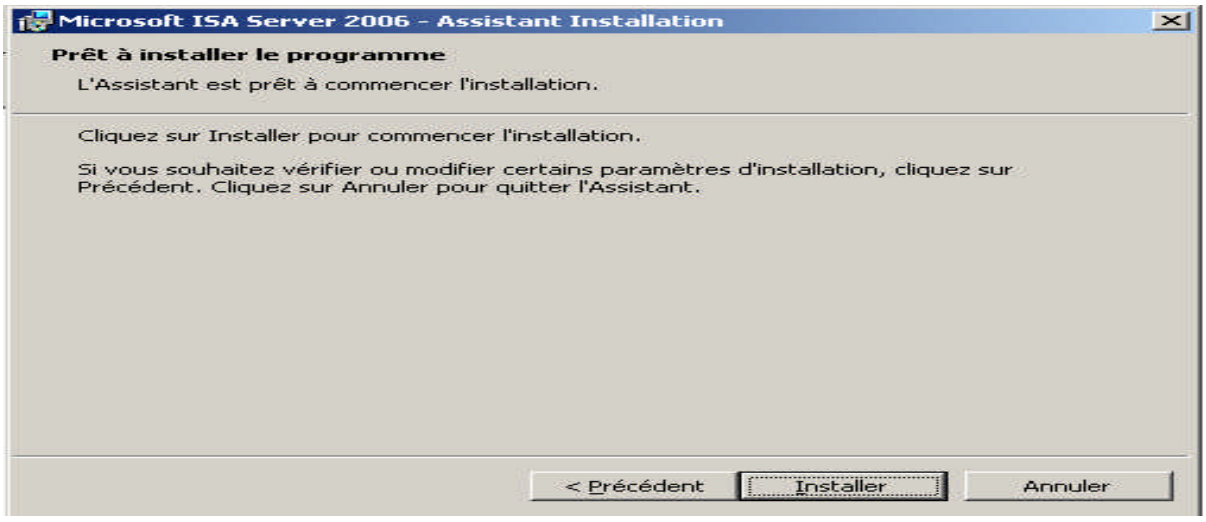
On clique sur suivant et un message d'avertissement qui indique qu'ISA Server 2006 accepte les connexions des clients de pare-feu pour lesquels le chiffrement n'est pas pris en charge



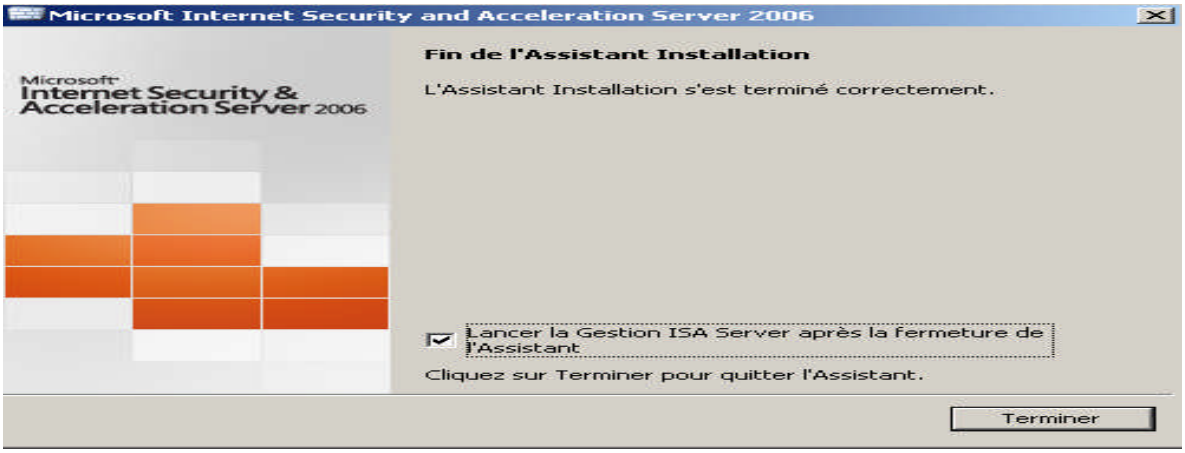
On cochant cette case on peut autoriser des ordinateurs qui exécutent des versions précédentes du client (exp ISA 2004) et on clique sur suivant



Cette figure nous indique que certains services s'exécutant localement sur cette machine peuvent être redémarrés ou désactivés, on clique sur suivant



On clique sur installer; l'installation va prendre quelques minutes tout dépend de la puissance de la machine

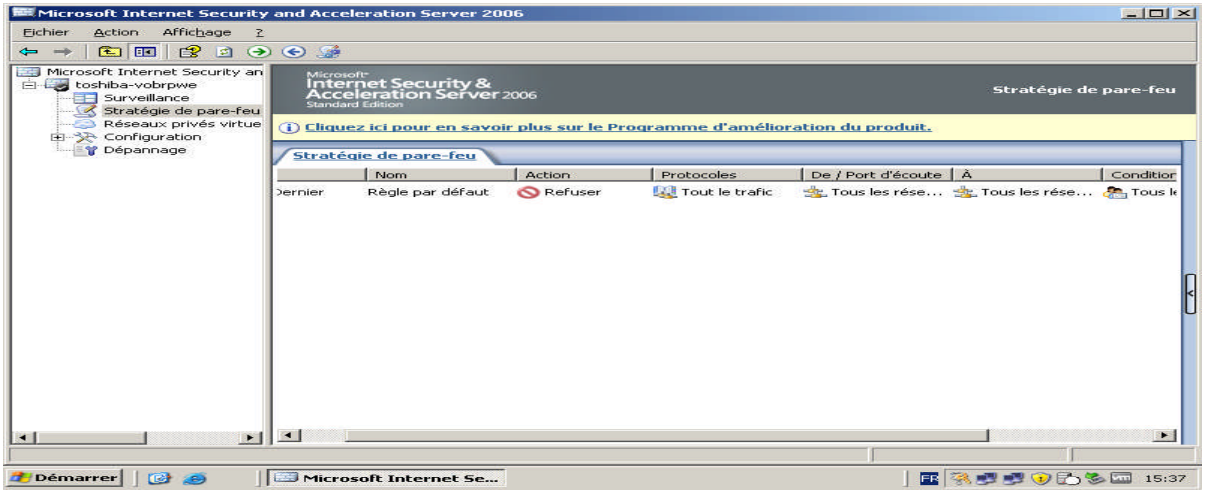


On clique sur Terminer et la gestion ISA Server se lance juste après la fermeture de l'assistant.

Apres l'installation du ISA server on effectue les taches suivantes :

- ✓ Création de la règle d'accès (http, https, FTP) vers internet depuis le réseau local.
- ✓ Paramétrage des règles systèmes et des règles d'accès ISA.
- ✓ Création des règles d'accès SMTP et de publication pour Exchange.

III.7.4 création des règles d'accès

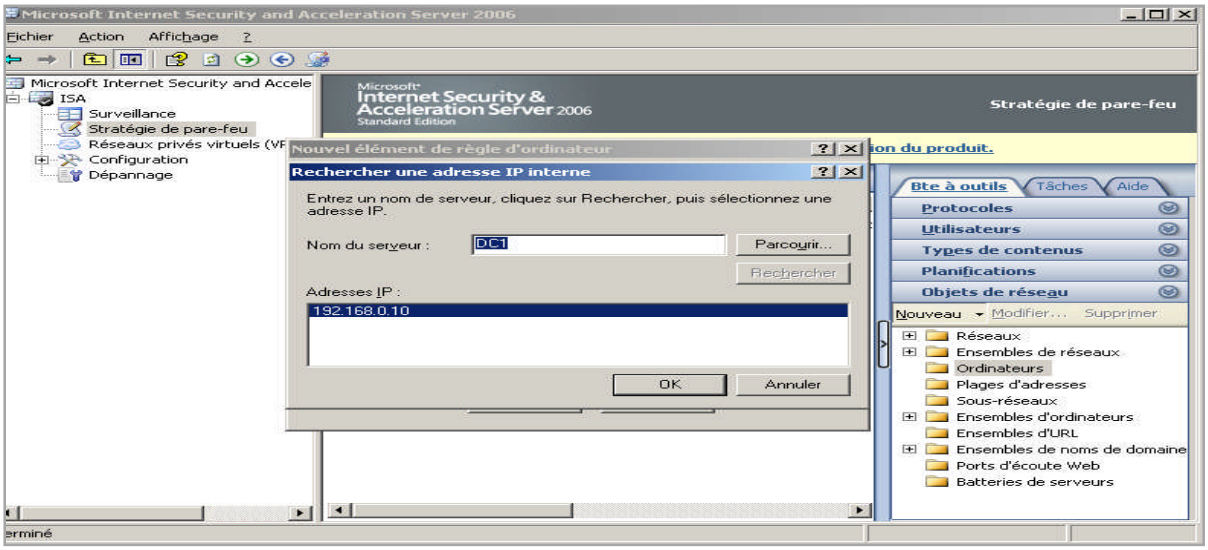


La première et seule règle qui existe par défaut au niveau du serveur ISA est celle qui dit que tout le trafic est refusé depuis tous les réseaux à destination de tous les réseaux, donc il faut autoriser les trafics supplémentaires

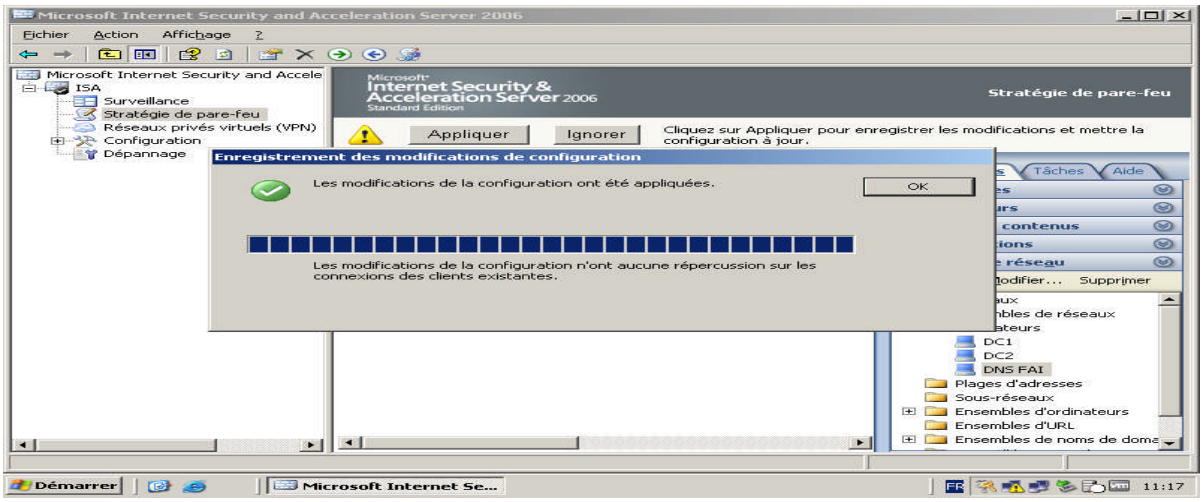
III.7.4.1 Création de la règle d'accès DNS

Notre objectif est d'ouvrir le flux DNS depuis les deux serveurs DNS qui sont hébergés sur les machines DC1 et DC2 et autoriser ces machines à renvoyer des requêtes DNS à l'extérieur à destination des serveurs DNS du fournisseur d'accès.

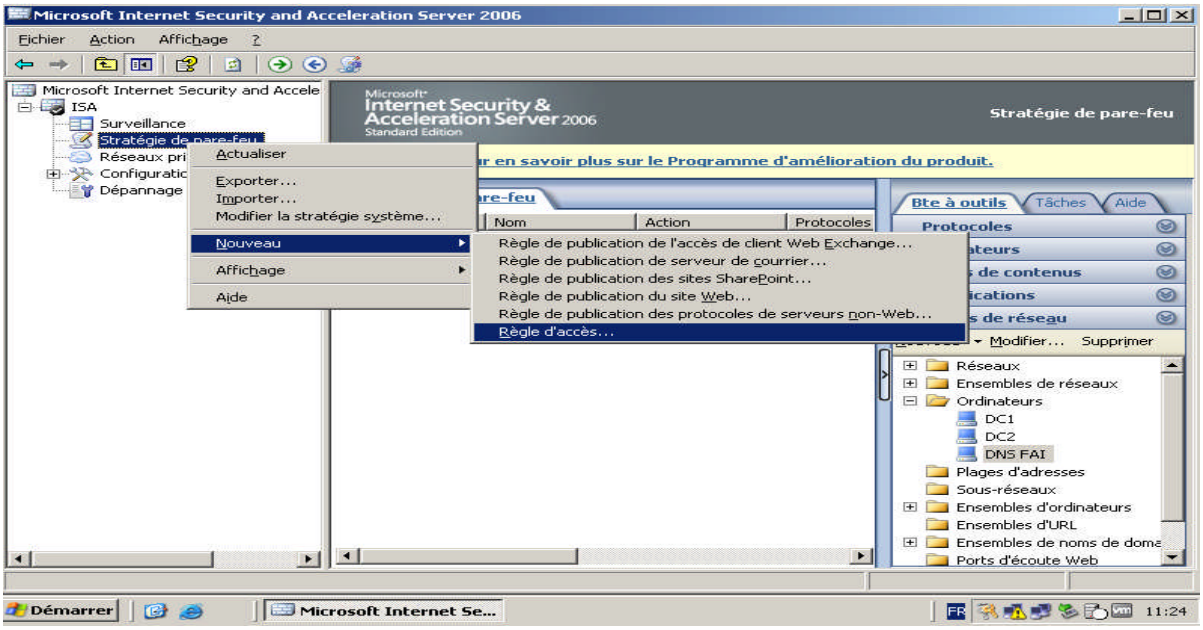
On ouvre le volet des taches et on va créer des nouveaux objets, trois nouveaux ordinateurs ; le premier s'appellera DC1 et le deuxième s'appellera CD2 et le troisième DNS FAI

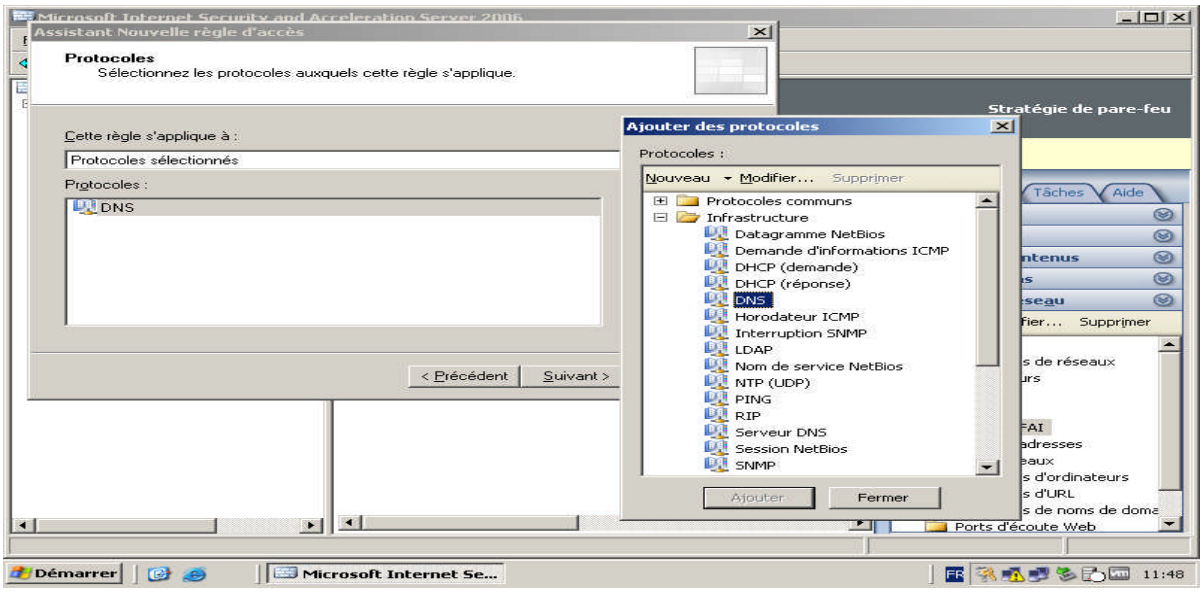


Et on clique sur appliquer pour valider les modifications

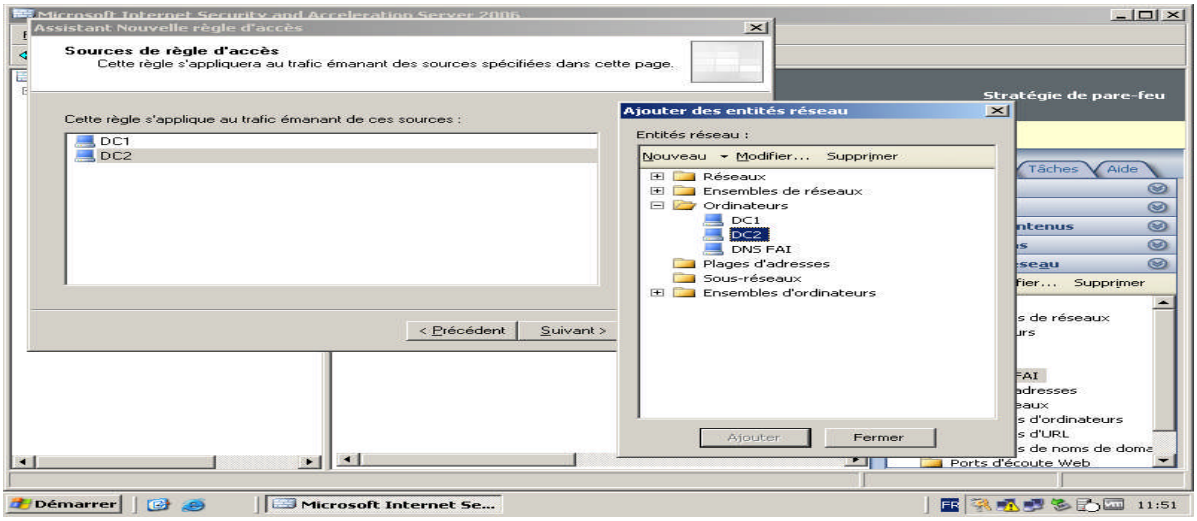


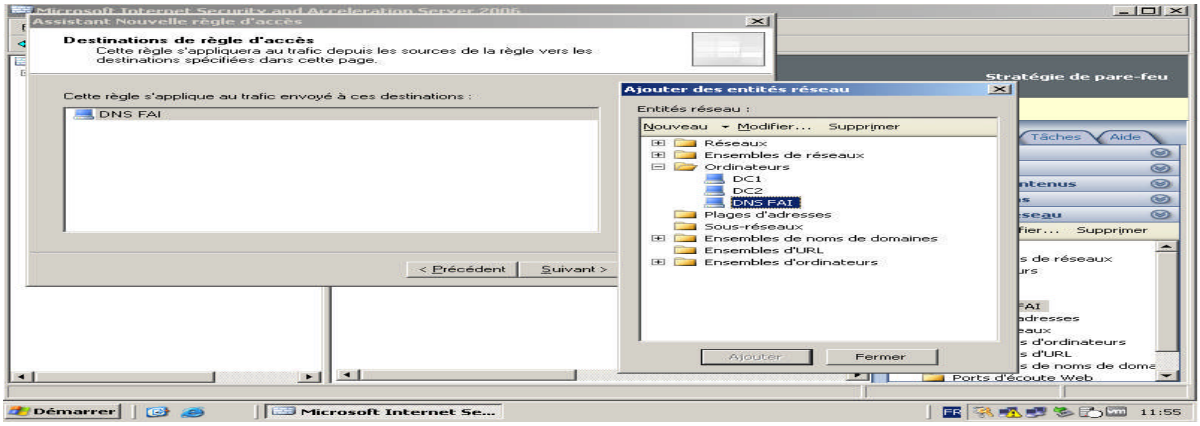
Et maintenant on peut créer notre règle d'accès dans stratégie de pare-feu, bouton droit, nouveau, règle d'accès comme le montre la figure suivante



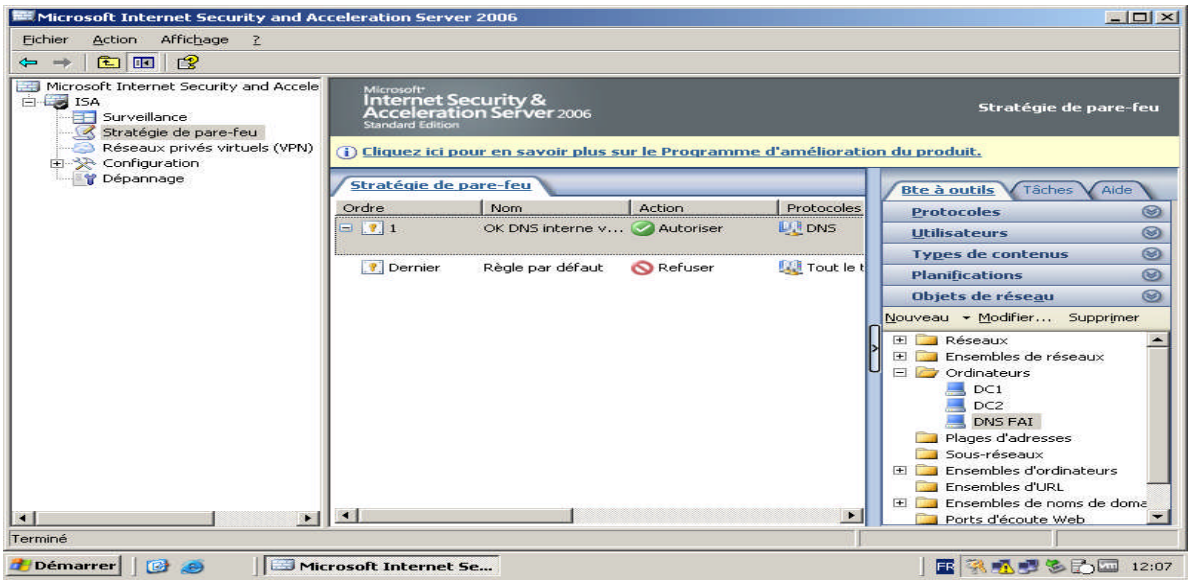


Cette règle s'appliquera au trafic émanant des serveurs DC1 et DC2 vers le DNS FAI





Cette règle va s'appliquer sur tous les utilisateurs, et on clique sur terminer et on la valide en cliquant sur appliquer.



Vérification :

Ouvrir une fenêtre de commande et on ping sur le site de Microsoft www.microsoft.com

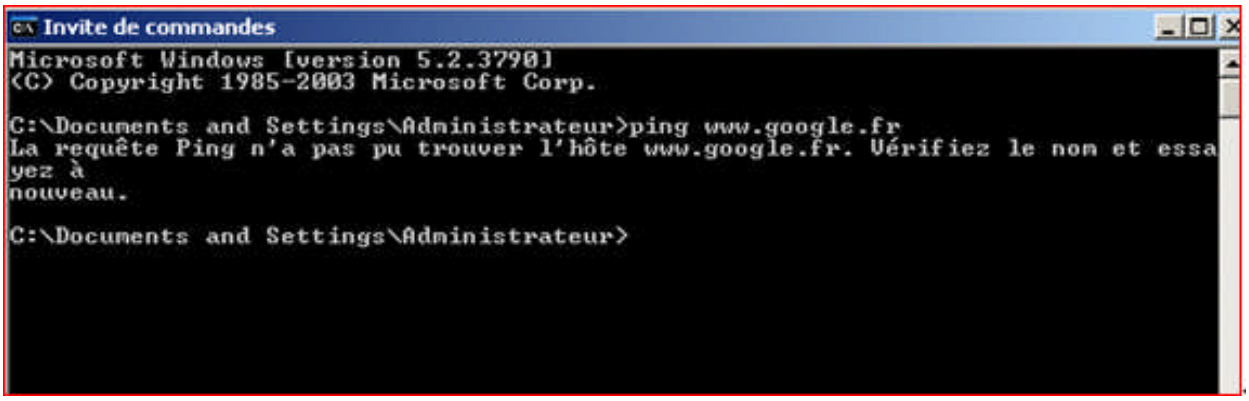
```
c:\>ping www.microsoft.com

Envoi d'une requête 'ping' sur lb1.www.ms.akadns.net [207.46.225.6
ets de données :

Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 207.46.225.60:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

c:\>
```

La résolution du DNS fonctionne très bien, et on voie l'adresse IP du ce site.

III.7.4.2 Création de la règle d'accès (http, https, FTP)

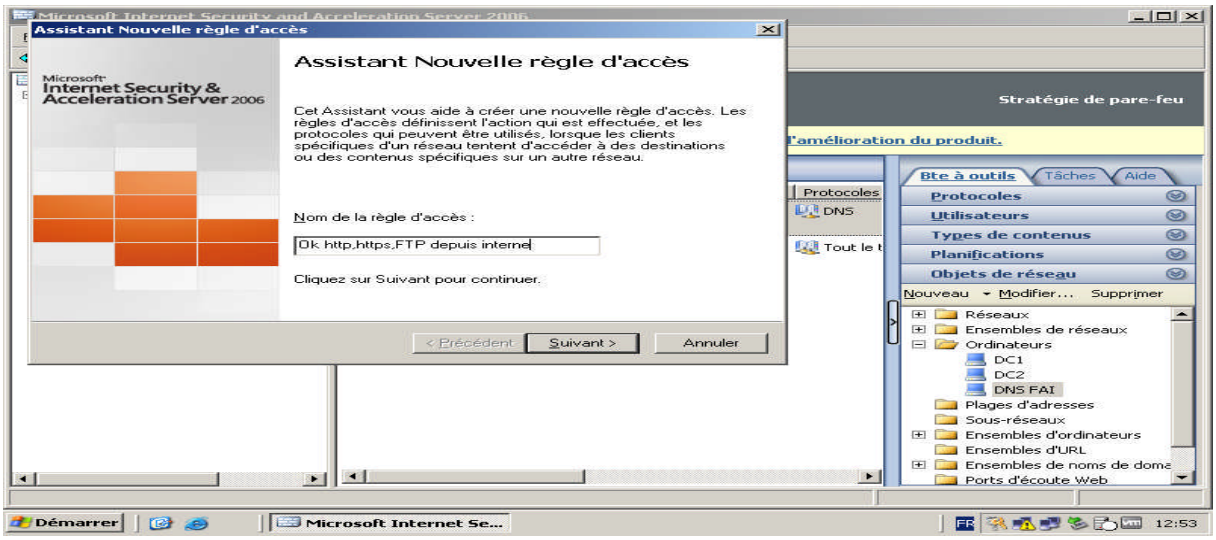
Cette règle d'accès permet aux ordinateurs du réseau interne de se connecter à internet au travers du protocole comme http, https et encore FTP depuis le réseau local.

Test avant la création de la règle :



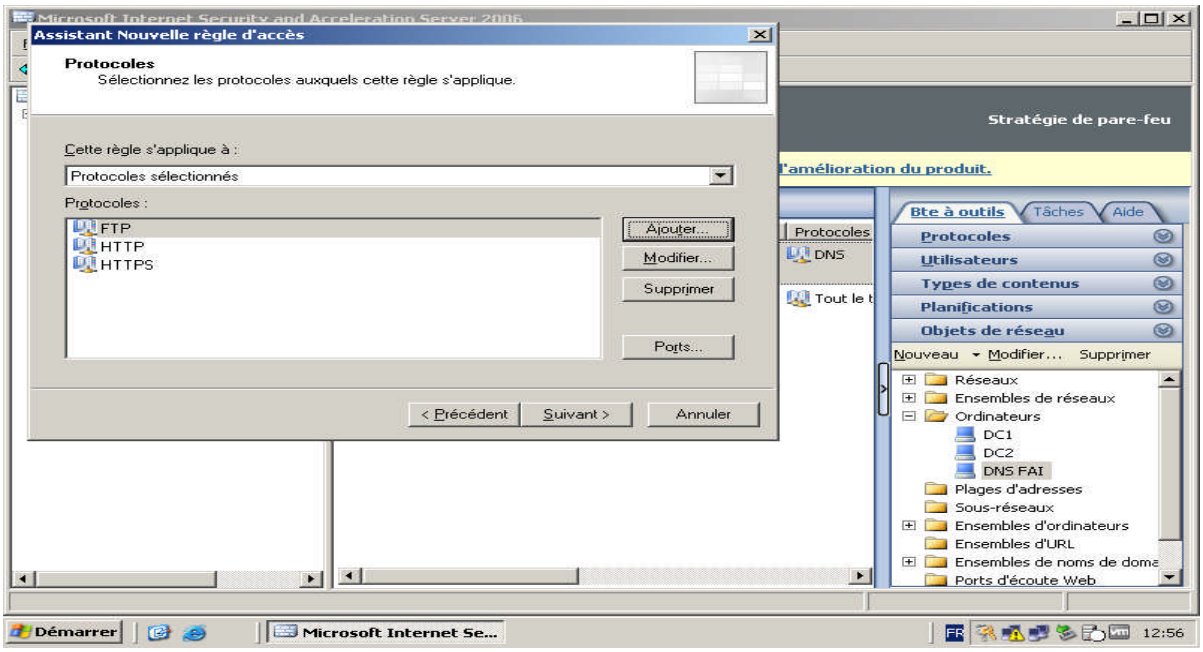
Le ping est échoué car le ISA bloque tout le trafic par défaut.

Pour créer la règle d'accès qui autorise ce trafic on suit les étapes suivantes :

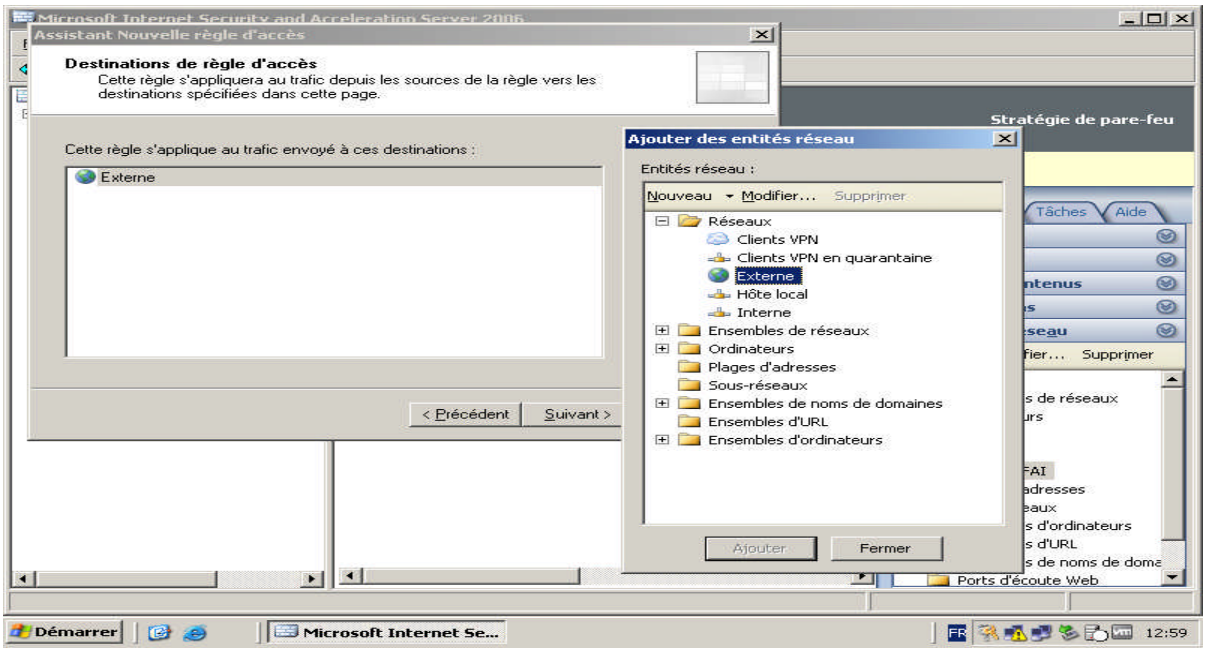


L'assistant de nouvelle règle d'accès s'ouvre, on lui effectue le nom « Ok HTTP, HTTPS, FTP depuis le réseau interne », puis on clique sur suivant.

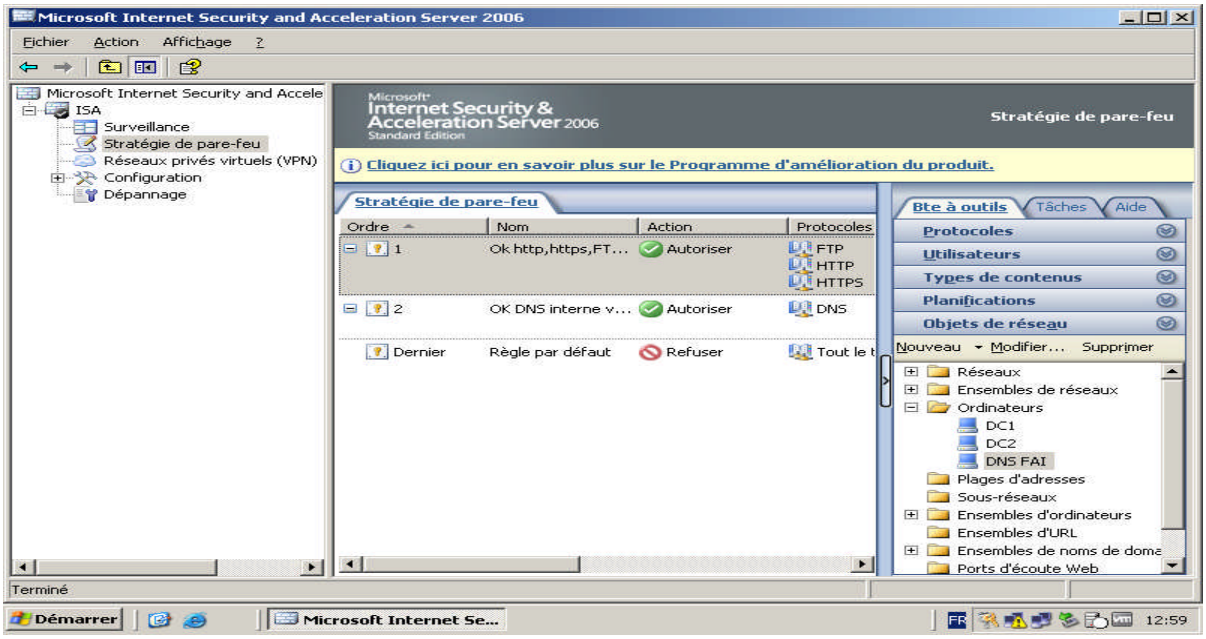
Cette règle n'autorise pas tous le trafic mais des protocoles sélectionnés; HTTP, HTTPS et le protocole de transfert des fichiers FTP



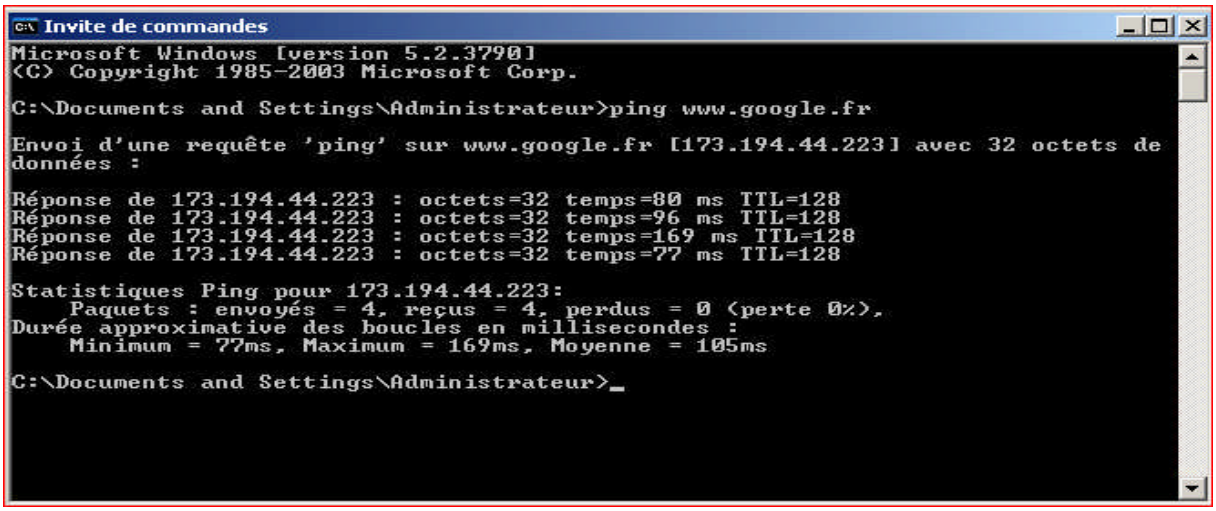
On clique sur suivant, une nouvelle fenêtre s'ouvre dont on indique la source du trafic qui est le réseau interne émanant à destination du réseau externe, on clique sur suivant



Notre règle est maintenant terminée, il suffit juste de cliquer sur appliquer pour la valider



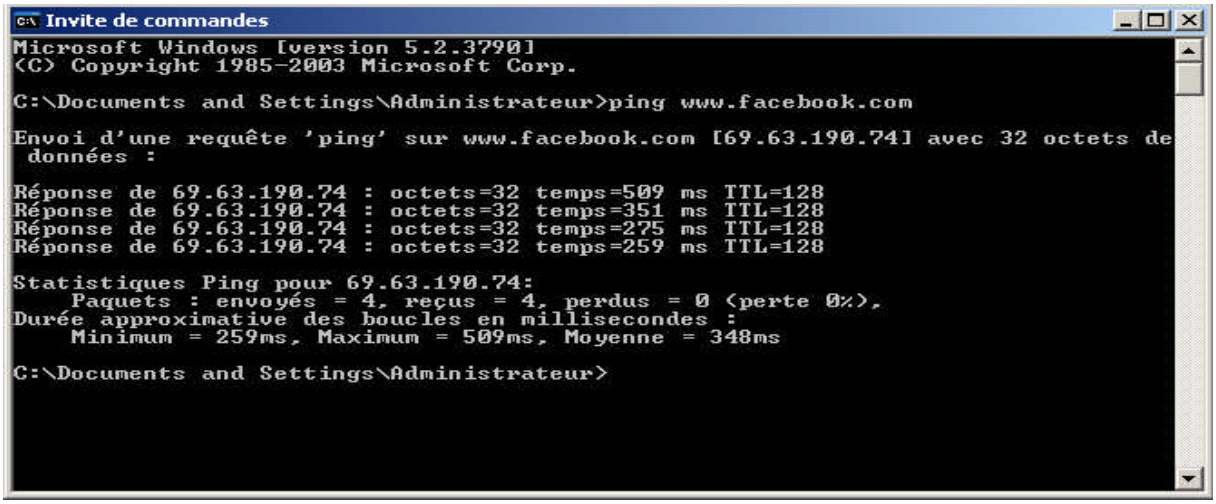
Test après la création de la règle :



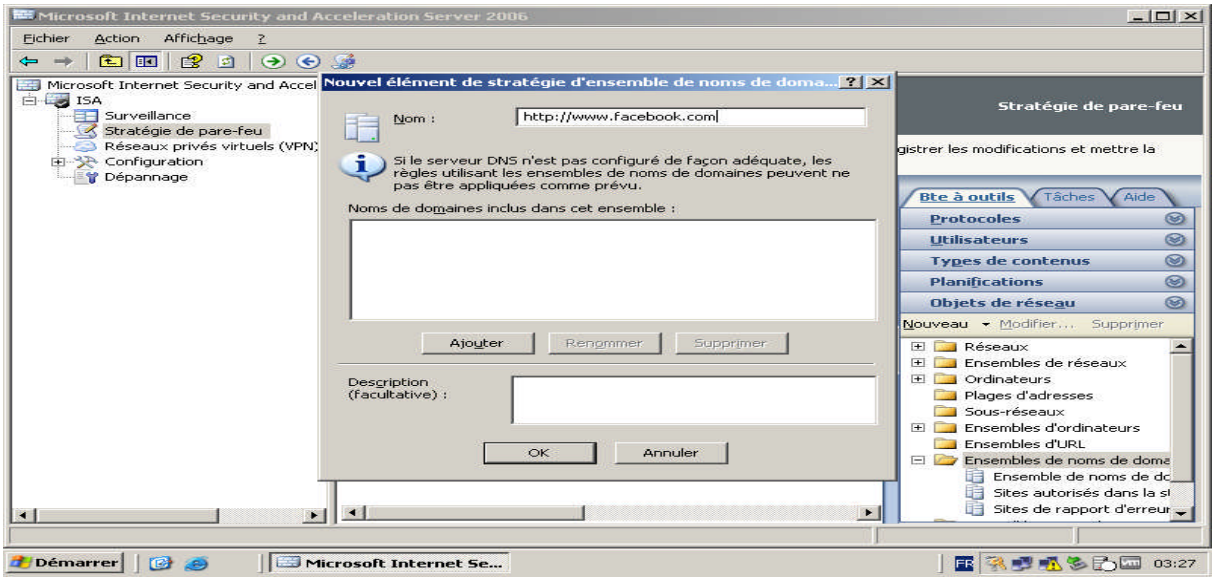
III.7.4.3 Création de la règle qui refuse un site web

Cette règle d'accès empêche les ordinateurs du réseau interne de se connecter au site web (www.facebook.com).

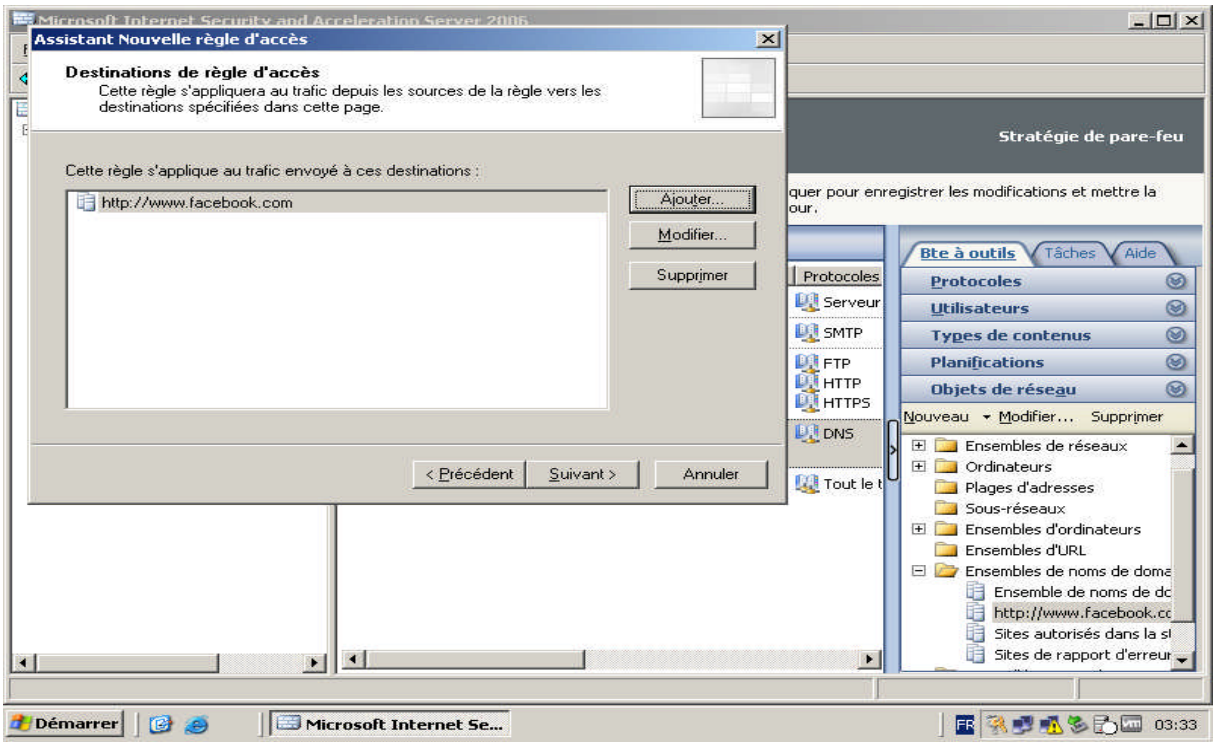
Test avant la création de la règle :



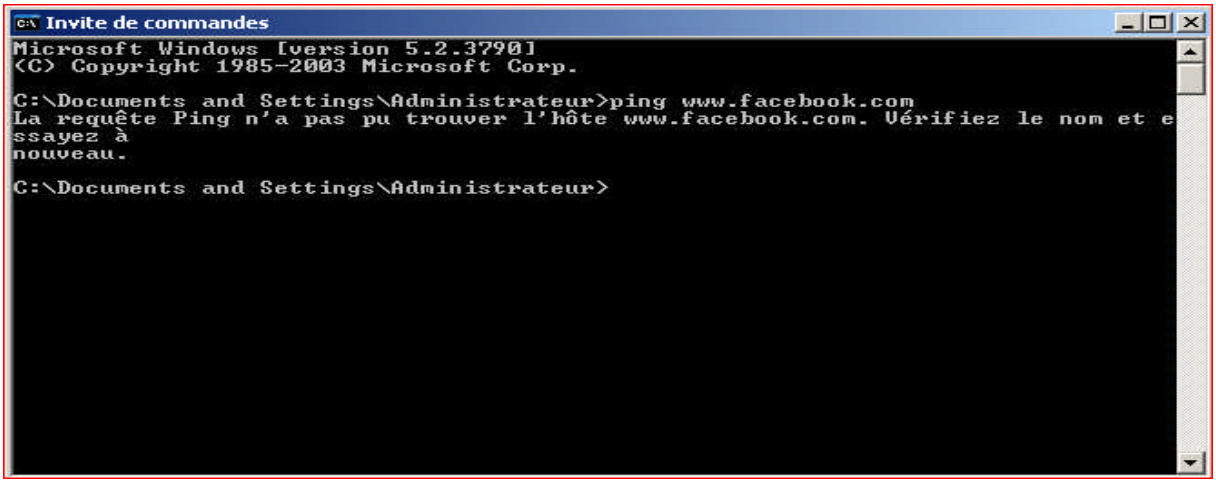
Pour créer la règle d'accès qui bloque ce trafic on doit d'abord indiquer le site (www.google .com) dans l'ensemble de nom domaine



Après avoir nommé cette règle, on sélectionne le protocole http puis on choisit la source du trafic (interne) vers la destination (www.facebook.com)



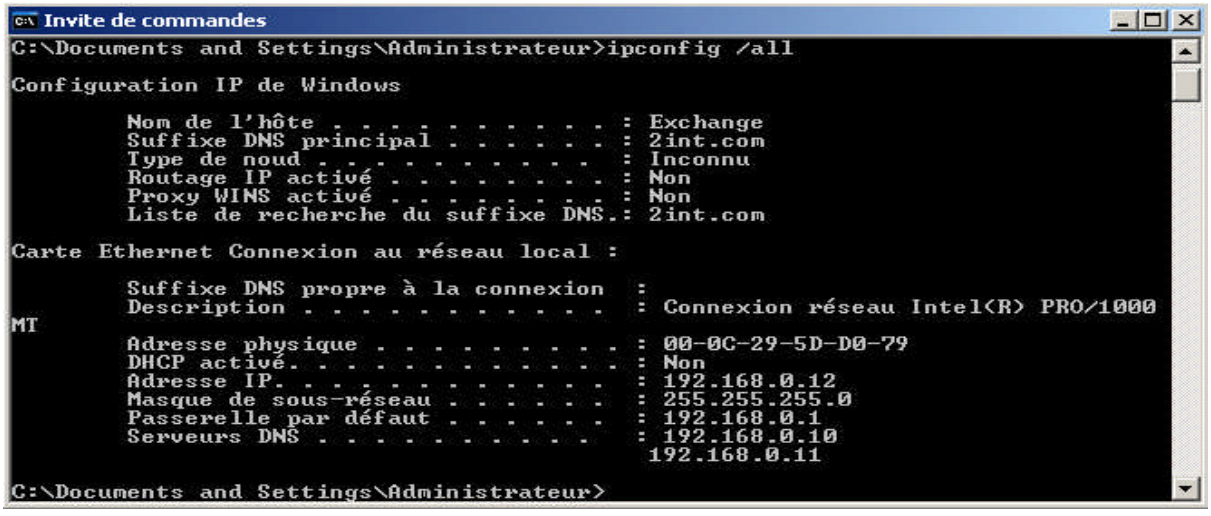
Test : après avoir validé la règle, on ping le site www.facebook.com dans la fenêtre d'invite de commande :



Le ping n'a pas pu trouver l'hôte www.facebook.com.

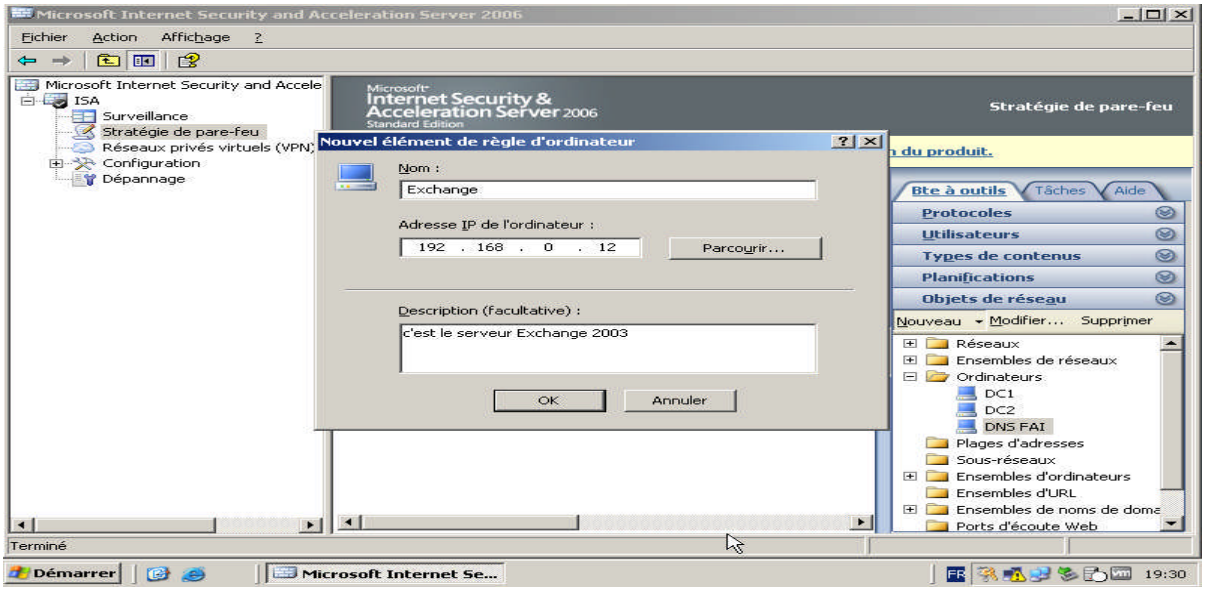
III.7.4.4 Création des règles d'accès SMTP et de publication pour Exchange

Après avoir installé le Serveur de messagerie électronique Exchange 2003 dans une autre machine virtuelle qui doit être intégrée dans le domaine d'Active Directory. Voici ces paramètres réseau :



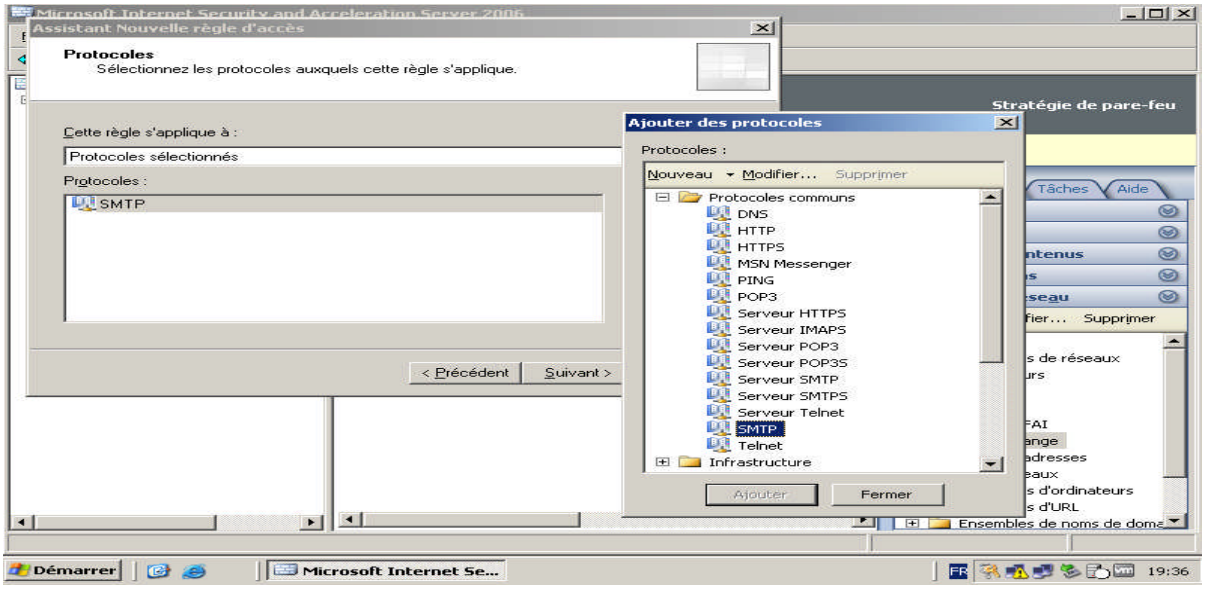
Dans notre application, on s'intéresse aux règles de publication de ce dernier en toute sécurité avec le ISA. Et pour cela on crée une règle dont on configure les accès sur le ISA Server afin que le serveur Exchange SMTP puisse envoyer des messages sur internet et de l'autre coté les recevoir depuis internet.

Avant de créer ces règles on crée un nouvel objet de type ordinateur on lui effectue le nom « Exchange », une adresse IP et une description comme le montre la figure suivante :

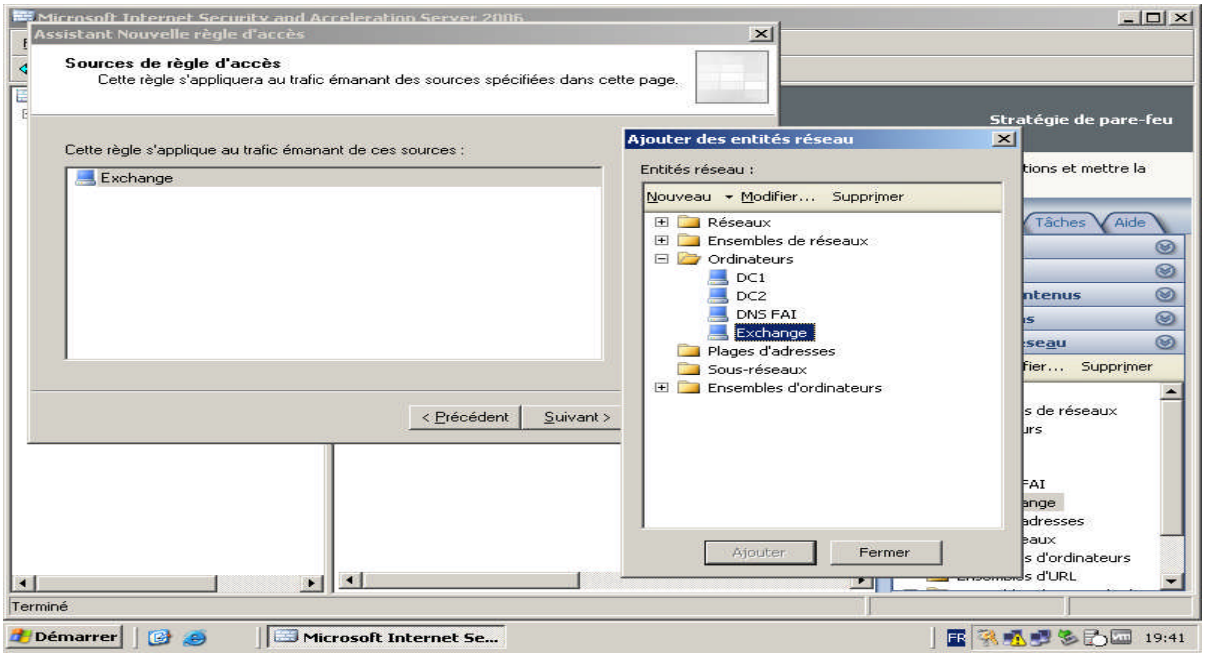


Maintenant on va créer la première règle qui permette à ISA Server d'envoyer des messages SMTP du réseau intranet vers l'internet

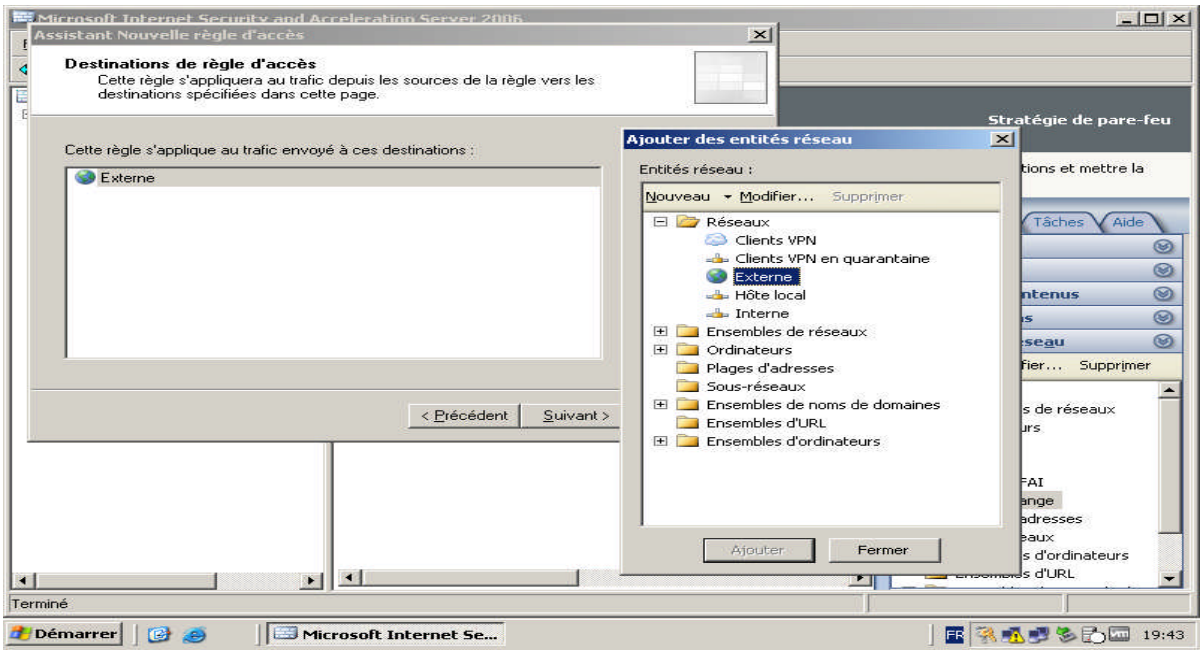
Cette règle est une règle de sortie (règle d'accès) qui porte le nom « Ok SMTP sortant pour Exchange », elle autorise un trafic qu'on sélectionne en cliquant sur ajouter et dans les protocoles commun on sélectionne le protocole SMTP



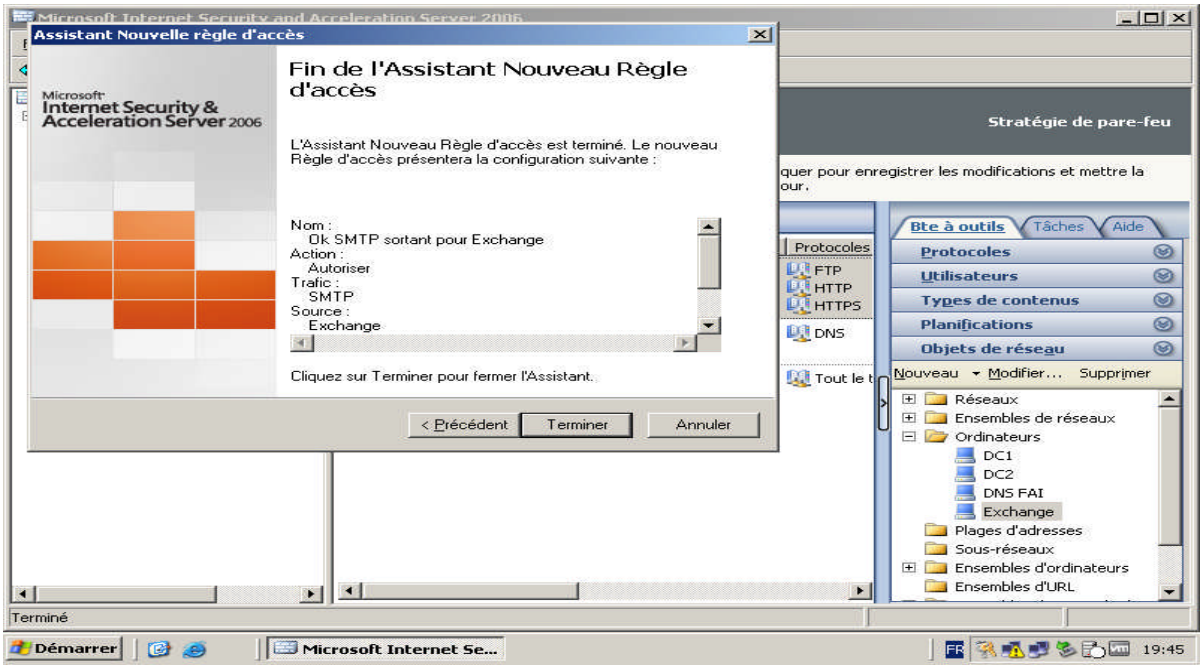
On clique sur suivant, une nouvelle fenêtre apparait pour indiquer que cette règle s'applique au trafic émanant du ISA et on sélectionne l'objet à autoriser qui nous intéresse c'est bien « Exchange »



On sélectionne l'objet et on clique sur suivant, puis on sélectionne la destination de ce trafic qui est le réseau externe (internet)



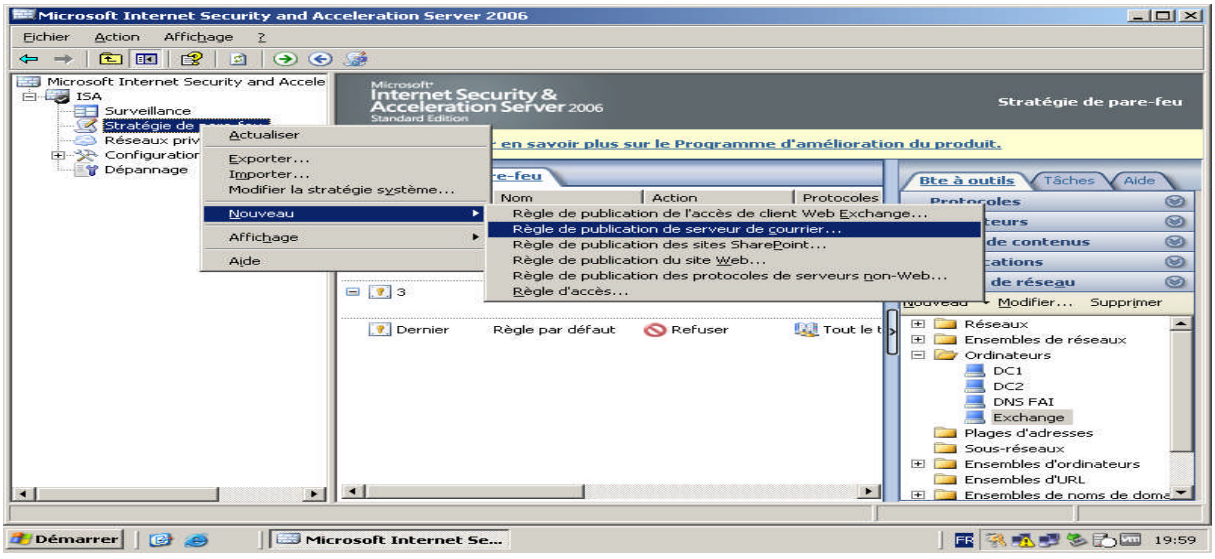
Une fenêtre apparait, elle contient le résumé de cette règle et on clique sur terminer puis sur appliquer.



La création de la première règle est réalisée et on passe maintenant à la création de la deuxième règle.

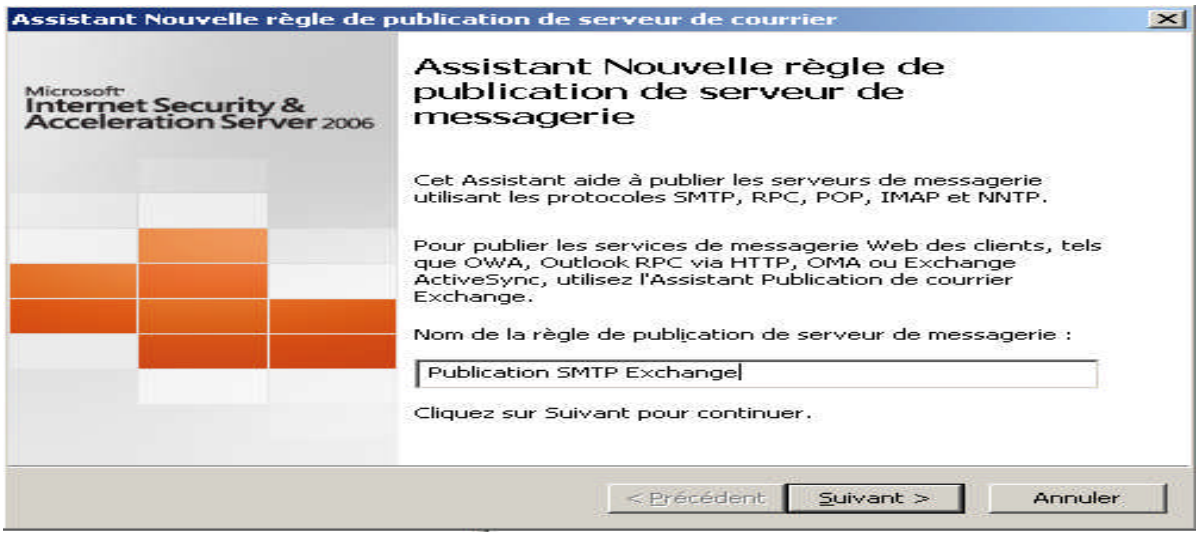
Création de la règle de publication du serveur Exchange :

Pour créer cette règle on ouvre la console de gestion d'ISA Server et dans la stratégie de pare-feu, bouton droit on sélectionne une nouvelle règle de publication de serveur de courrier

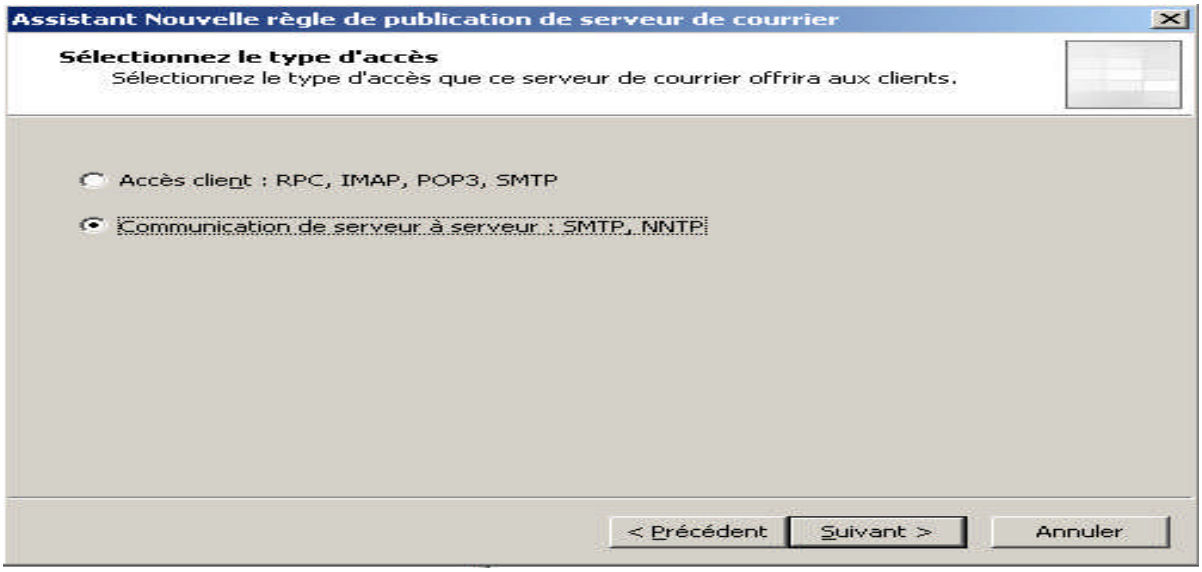


L'assistant nouvelle règle de publication de serveur de messagerie s'ouvre qui va permettre d'exposer le serveur Exchange au niveau internet d'une manière complètement sécurisée.

Cette règle porte le nom « Publication SMTP Exchange »

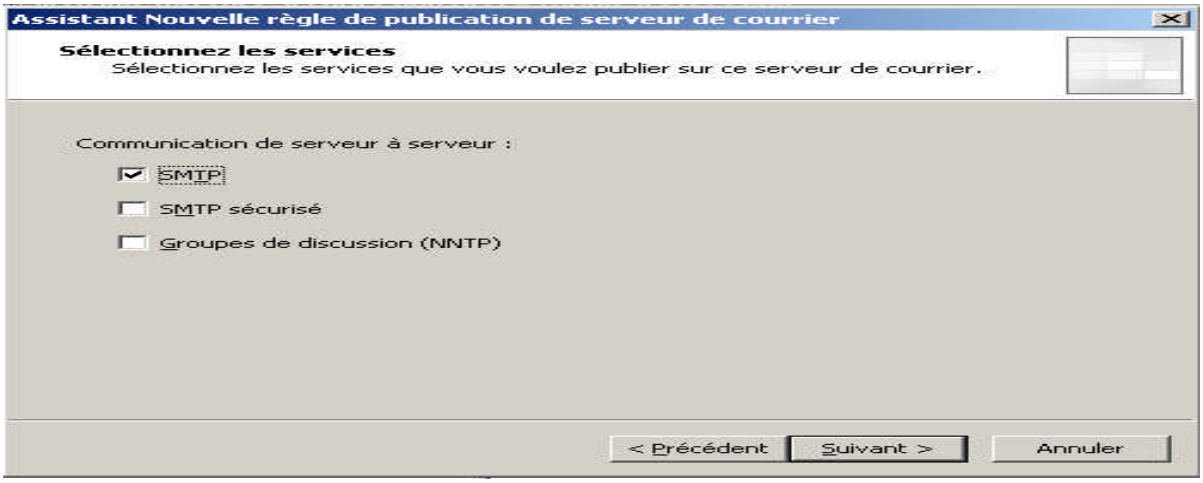


On clique sur suivant, une nouvelle fenêtre s'ouvre pour sélectionner le type d'accès

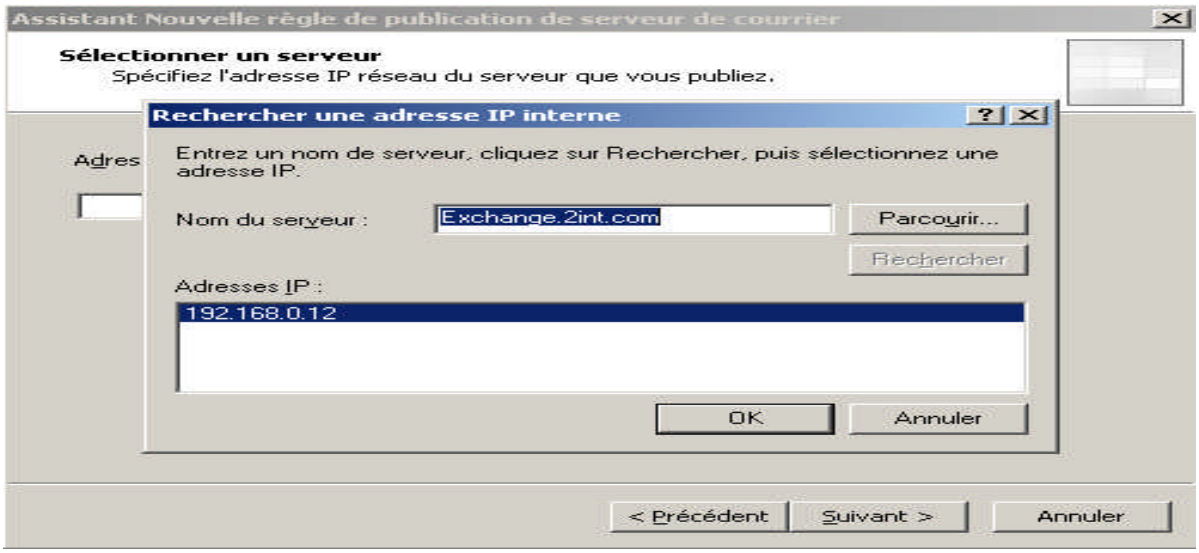


Le type de cette communication est « communication de serveur à serveur » car le serveur exchange envoie des courriers électroniques aux autres serveurs SMTP connectés sur internet.

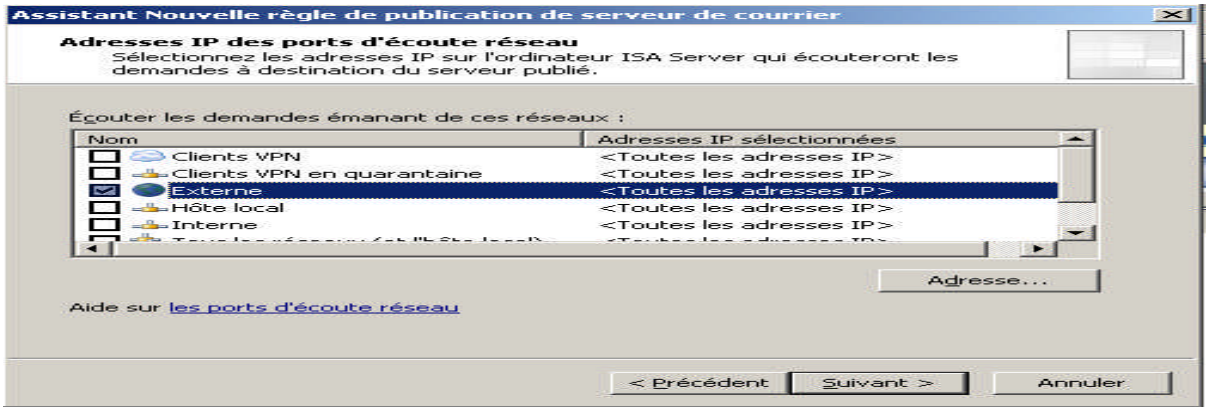
On clique sur suivant, une nouvelle fenêtre s'ouvre pour sélectionner les services à publier sur notre serveur



La communication de serveur à serveur est de type SMTP, on clique sur suivant et on donne l'adresse IP du serveur Exchange.



On clique sur Ok puis suivant, une nouvelle fenêtre s'ouvre pour sélectionner les adresses IP qui écoutent les demandes à destination d'Exchange.



On écoute les demandes émanant sur le réseau externe, sur lequel le serveur ISA va publier pour se faire passer le serveur SMTP Exchange, et on clique sur suivant

La création de cette règle est réalisée, on clique sur terminer puis sur appliquer pour la valider.

III.8 Conclusion

La connexion de réseaux et d'utilisateurs à Internet soulève des questions de sécurité et de productivité. ISA Server offre aux entreprises une connectivité Internet sécurisée et rapide, exploitant les puissantes fonctions de gestion de Windows 2003. Il apporte aux entreprises des capacités complètes de contrôle d'accès et de surveillance d'utilisation comme il protège les réseaux contre les accès frauduleux, inspecte le trafic et alerte les administrateurs en cas d'attaque.

Les organisations qui souhaitent ouvrir leurs réseaux à Internet doivent considérer ISA Server comme une composante stratégique de leur infrastructure de communication.

Conclusion générale

Conclusion générale

La sécurité du système d'information d'une entreprise est un requis important pour la poursuite de ses activités. Qu'il s'agisse du vol de ses secrets de fabrication ou de la perte de ses données clients, et ça nous a ramené à parler de la nécessité de garantir certains besoins de sécurisation : l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que la non répudiation des actes.

Dans notre mémoire nous nous sommes intéressés à l'installation et la configuration du pare-feu ISA Server dans le but de faire faces aux différents actes de malveillance dont la nature et la méthode d'intrusions sont sans cesse changeantes.

Le ISA Server propose un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau.

Ce projet nous a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il nous a initiés au monde de la recherche sur les réseaux surtout en ce qui concerne la sécurité. Il nous a également permis de découvrir le logiciel de simulation VMware Worktation, Windows Server 2003, service d'annuaire Active Directory et Microsoft Exchange 2006.

Dans les grandes entreprises le ISA seul reste insuffisant pour garantir la sécurité de ses ressources, alors il est nécessaire de l'inclure dans une démarche qui prendra en compte d'autres paramètres tel que des pare-feux matériels, des anti-virus, ainsi des mises à jour leurs applications.

Annexe

Annexe

VMware Workstation

VMware Workstation est un logiciel permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

Windows server 2003

Windows Server 2003 est un système d'exploitation orienté serveur développé par Microsoft. Il est considéré par Microsoft comme étant la pierre angulaire de la ligne de produits serveurs professionnels Windows Server System. Selon Microsoft, Windows Server 2003 est plus évolutif et fournit de meilleures performances que son prédécesseur Windows Server 2000.

Parmi les produits de la famille Windows 2003, il existe quatre systèmes d'exploitation : Windows 2003 Web, Windows 2003 Standard, Windows 2003 Enterprise et Windows 2003 Datacenter.

Active Directory

Active Directory sert d'annuaire des objets du réseau, il permet aux utilisateurs de localiser, de gérer et d'utiliser facilement les ressources. Il permet de réaliser la gestion des objets sans liens avec la disposition réelle ou les protocoles réseaux employés. Active Directory organise l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets.
Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants d'une façon complètement centralisée.

Active Directory permet :

- **Une administration simplifiée :** Active Directory offre une administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.
- **Une mise à l'échelle :** Active Directory permet de gérer des millions d'objets répartis sur plusieurs sites si cela est nécessaire.
- **Un support standard ouvert :** Active Directory utilise DNS pour nommer et localiser des ressources, ainsi les noms de domaine Windows 2003 sont aussi des noms de domaine DNS.

Active Directory fonctionne avec des services de clients différents tels que NDS de Novell. Cela signifie qu'il peut chercher les ressources au travers d'une fenêtre d'un navigateur web. De plus, le support de Kerberos 5 apporte la compatibilité avec les autres produits qui utilisent le même mécanisme d'authentification.

Microsoft Exchange Server 2003

Exchange est le produit de collaboration basé sur le courrier électronique le plus utilisé par les entreprises. Certains paramètres ont été améliorés afin de rendre Exchange Server 2003 plus performants dans le monde de l'entreprise. Microsoft a élargie et renforcé les fonctionnalités de connexions au système de messagerie Exchange Server 2003. Dorénavant, les utilisateurs peuvent bénéficier de 4 modes connexions : Outlook 2003, Outlook Web Access, Exchange Server ActiveSync, Outlook Mobile Access.

Bibliographie

Bibliographie

[1] J.F. Pillou « Tout sur la sécurité informatique », Ed. Dunod, 2005.

[2] J.F. Pillou « Tout sur les réseaux et internet », Ed. Dunod, 2007.

[3] T. Shinder's « ISA 2006 Migration Guide », Ed.Syngress, 2006.

[4] K. Stiti , S.Bellouni « Sécurité des données par la cryptographie quantique », mémoire de Master en électronique, UMMTO, 2011.

[5] K. Meksem, L. Menad « Conception d'une interface de configuration d'un serveur SSH sous Windows XP », mémoire de Master en électronique, UMMTO, 2011.

[6] M. Lebik, T. Rennou « Mise en place d'un serveur de Messagerie Intranet », mémoire d'ingénieur d'état informatique, UMMTO, 2010.

[7] S. Aliche, A. Haddad « Implémentation d'une politique de sécurité au niveau de département informatique de l'entreprise ENIEM de Tizi-Ouzou », mémoire de Master en électronique, UMMTO, 2011.

[8] Y. Douicher, S. Sissoko « Mise en place d'un pare-feu en utilisant le Smoothwall », mémoire de Master en électronique, UMMTO, 2012.

[9] M. Horri, D. Ameziane « Sécurité des réseaux mobiles multimédia », mémoire d'ingénieur d'état en télécommunication, IT Oran, 2005.

[10] http://www.google.fr/le réseau informatique.

[11] http://www.google.fr/la sécurité des réseaux dans les entreprises.

[12] http://www.google.fr/présentation de ISA server (module18).

[13] http://www.google.fr/information dans une entreprises par le firewall isa server (livre blanc Microsoft).

[14] http://www.google.fr/ISA server édition entreprise.

[15] http://www.google.fr/ISA server édition standard.

[16] http://www.microsoft.com.

GLOSSAIRE

Glossaire

ACL Access Control List

ARP Address Resolution Protocol

COM Component Object Model

DES Data Encryption Standard

DMZ Demilitarized Zone

DNS Domain Name System

DOS Disk Operating System

FDDI Fiber Distributed Data Interface

FTP File Transport Protocol

FTS File Transfer Service

HTTP HyperText Transfert Protocol

HTTP-S HyperText Transfert Protocol Secure

ICMP Internet Control Message Protocol

IP Internet Protocol

ISA Internet Security and Acceleration

ISO International Standard Organization

LAN Local Area Network

LDAP Light weight Distributed Data Interface

MAC Media Access Control

MAN Metropolitain Area Network

MITM Man In The Middle

NAT Network Interface Card

NTLM NT Lan Manager

Glossaire

OSI Open Systems Interconnection

POP Post Office Protocol

PPP Protocol Point-To-Point

POP3 Post Office Protocol version 3

QOS Quality Of Service

RADIUS Remote Authentification Dial In User Service

RARP Reverse Address Resolution Protocol

RRAS Routing and Remote Access Service

SDK Software Development Kit

SMTP Simple Mail Transfer Protocol

SSH Secure Shell

SSL Secure Socket Layer

SSO Single Sign-On

TCP Transfer Control Protocol

UDP User Datagram Protocol

VPN Virtual Private Network

WAN Wide Area Network

WMT Windows Media Technology

Un réseau informatique est un ensemble de micro-ordinateurs interconnectés dans le but d'assurer le transfert de fichiers, le partage des ressources (imprimantes et données), l'exploitation de la messagerie ou l'exécution et la maintenance des programmes à distance.

Aujourd'hui les entreprises utilisent de plus en plus d'informations, ce qui nécessite une meilleure organisation et des conditions de stockage optimales. L'outil informatique joue un rôle primordial sur ce plan. Pour faciliter la transmission de ces données informatisées, les entreprises s'organisent autour d'un réseau.

La sécurité du système d'information d'une entreprise est un requis important pour la poursuite de ses activités. Qu'il s'agisse du vol de ses secrets de fabrication ou de la perte de ses données clients, et ça nous a ramené à parler de la nécessité de garantir certains besoins de sécurisation : l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que la non répudiation des actes.

Afin d'assurer un bon fonctionnement global de l'entreprise, on utilise une passerelle puissante et facile à administrer qui fournisse une connexion sécurisée tout en augmentant et améliorant les performances réseaux. ISA Server répond à ces exigences par la solution de connectivité Internet et le contrôle d'accès.