Les Dossiers

ABAQUE

Intranet - Dossier d'architecture

Version 3.0 - Janvier 2004

ABAQUE – *9 rue des Prévoyants de l'Avenir – 69003 Lyon – France*
SARL au capital de 50 000 Frs – 417 795 804 RCS Lyon / APE : 724Z

Tél. : (33) 06 11 19 55 52
Email : courrier@abaque.net
Web : www.abaque.net

TABLE DES MATIERES

1. INTRODUCTION

1.1. INTRANET ET COMMUNICATION D'ENTREPRISE

L'INTERNET et l'ensemble de la technologie qui en découlent sont en cours de radicalement modifier les architectures informatiques traditionnelles, tant dans les systèmes d'information des entreprises, que dans les méthodes de communication de ces entreprises avec l'extérieur (clients, prospects, partenaires, fournisseurs,...).
L'unanimité du marché autour de cette technologie et le dynamisme des différents acteurs à en repousser les limites, permettent d'envisager, à terme, que celle-ci offre un environnement de développement complet et standard. Toutefois, il semble plus prudent, aujourd'hui, dans le cadre d'applications de production, d'éviter de s'engager dans des choix et des solutions encore en pleine effervescence.

Par contre, il existe déjà dans l'entreprise de nombreuses activités pour lesquelles l'application de la technologie INTERNET dans le système d'information - ce que l'on appelle l'INTRANET, c'est à dire mettre les outils d'INTERNET à la disposition des utilisateurs dans les réseaux privés d'entreprise - amène de nombreuses opportunités, dont elle peut tirer profit.

Il s'agit principalement de tout ce qui concerne la diffusion, consultation, circulation, présentation, échanges d'informations de l'entreprise, de toutes sortes et de toutes origines (notamment non textuelles comme l'image, le son,...). Il s'agit d'un concept proche du Groupware que l'on pourrait appeler « **Système de Communication de l'Entreprise** ».

En effet, la réalité opérationnelle du concept INTRANET, dans ce domaine, est déjà illustré par de nombreuses références significatives, et les résultats des différents cabinets d'analyse lui assurent un succès rapide.

1.2. INTRANET EN TANT QUE FEDERATEUR

Néanmoins, ces premières mises en œuvre ne couvrent que le périmètre d'un établissement. La problématique de communication d'entreprise prend une nouvelle dimension lorsque l'on considère un groupe d'établissements. Et pourtant, là aussi la communication et la publication d'informations sont indispensables et importantes.

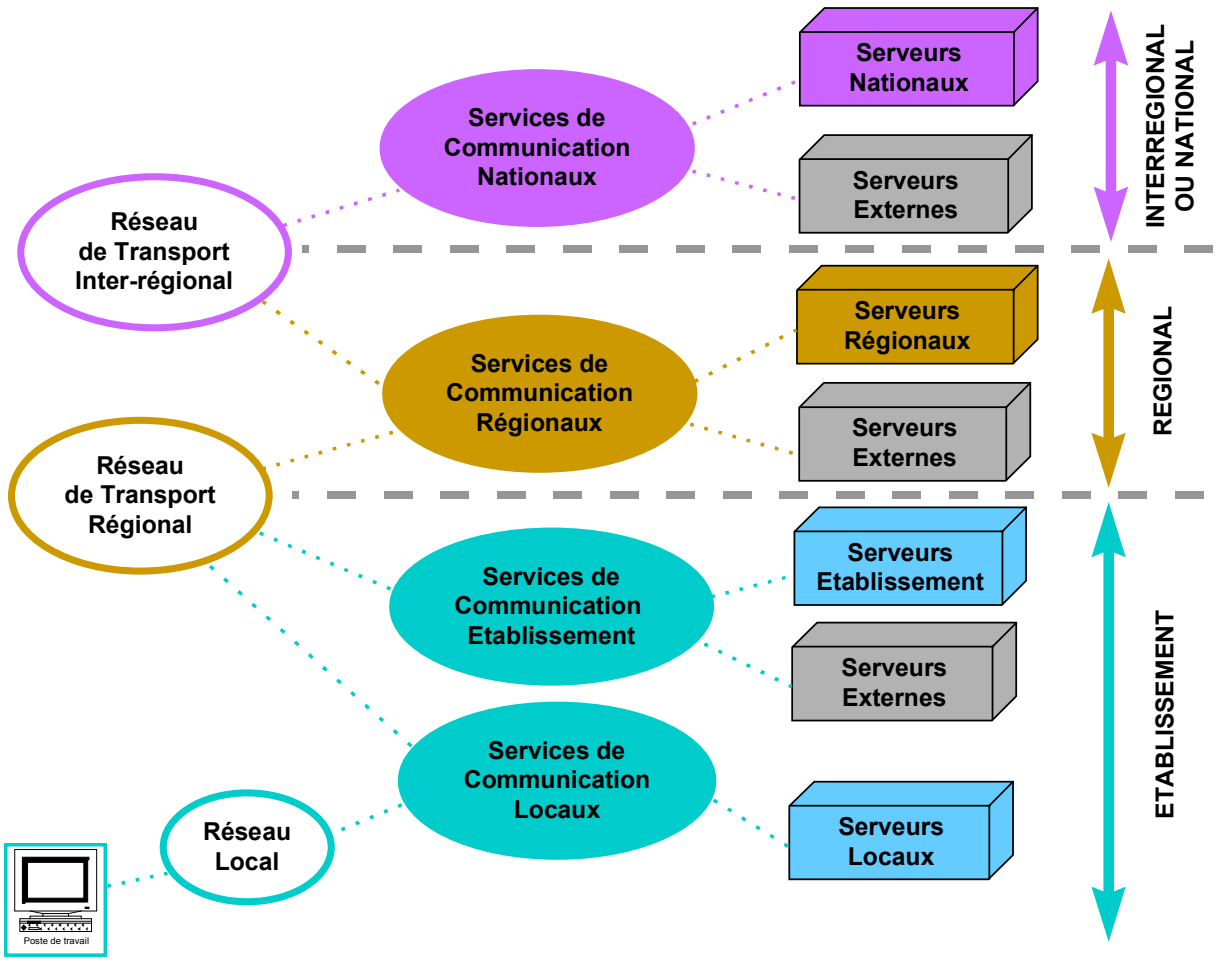
C'est pour cette raison qu'il est nécessaire de déployer une infrastructure technique et une organisation fédératrice permettant d'assurer des services de publication et de messagerie homogènes entre les établissements d'un Groupe.

Il est donc indispensable de bâtir une infrastructure permettant à chacun des serveurs d'être en relation avec l'ensemble des utilisateurs concernés du Groupe. C'est le rôle d'un Intranet fédérateur que de permettre cette mise en relation.

L'objectif de ce document est de présenter l'architecture technique de cette infrastructure fédératrice Intranet, et d'énoncer un certain nombre de règles et recommandations indispensables à la cohérence de l'ensemble : adressage, nommage, services, administration et sécurité.

2. ARCHITECTURE GENERALE

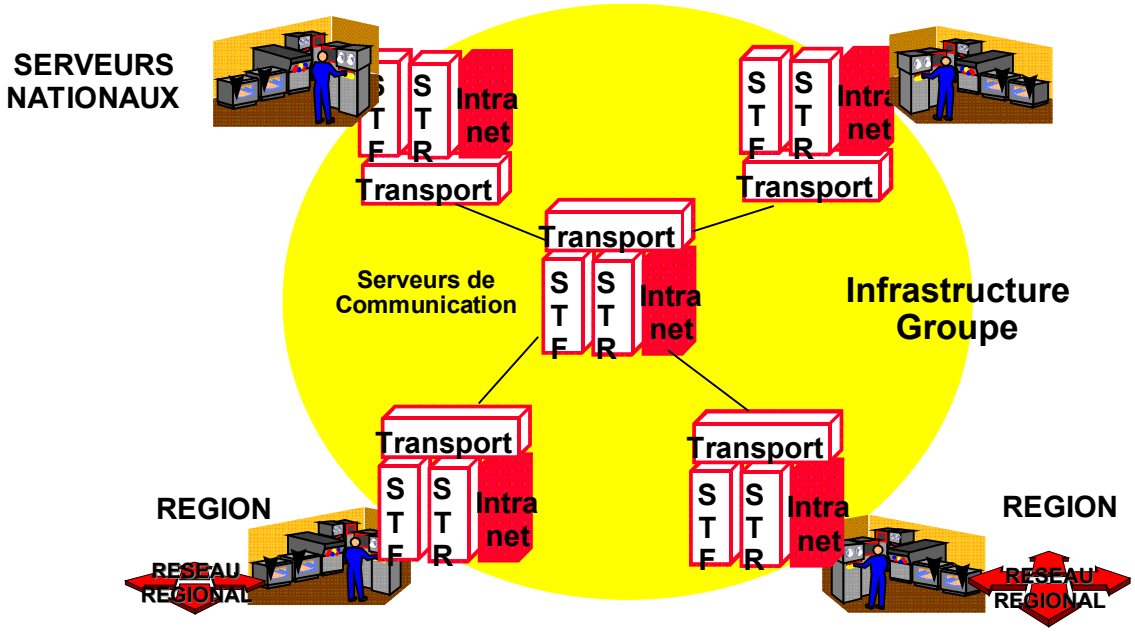
2.1. Rappel des règles de connectivité



2.2. Architecture générale cible

Cette organisation intègre, en particulier, un réseau de transport interrégional permettant à des services de communication nationaux et régionaux de dialoguer afin de véhiculer, de façon la plus pertinente possible, les flux d'informations entre les serveurs nationaux et les serveurs régionaux.

Le schéma général de l'infrastructure de communication d'un Groupe pourrait être la suivante :



L'infrastructure fédératrice constitue un nouveau service technique de communication, qui vient enrichir le développement de l'infrastructure de communication d'un Groupe.
Les fonctions de ce nouveau service sont, aujourd'hui, les suivantes :

- Service de messagerie Groupe
- Service de nommage IP (DNS)
- Service d'annuaire
- Service de publication d'information (Web)
- Service de partage d'information (News),

tout en intégrant les problématiques de sécurité et d'administration liées à ces services.

Remarque : la mise en œuvre d'Intranet répond de manière satisfaisante, aujourd'hui, à la problématique d'interconnexion de messageries et donc le service Intranet va englober et remplacer la solution de messagerie envisagée précédemment.

3. ARCHITECTURE DETAILLEE

3.1. Le pré-requis : l'infrastructure de transport IP

L'ensemble de protocoles TCP/IP représente le standard des services de transport de l'Internet. Sa mise en œuvre dans le cadre de l'infrastructure de transport est donc une condition nécessaire à la mise en place de services Intranet.
Le déploiement d'une infrastructure de transport en protocole IP, sécurisée et administrée, pour les services de communication inter-régionaux est indispensable.

Attention
La mise à disposition de services Intranet aux utilisateurs finaux nécessite le prolongement du protocole IP jusque dans chaque poste de travail.

- ***PLAN D'ADRESSAGE IP***

Afin d'assurer une cohérence d'adressage dans un Groupe, une entité doit définir et proposé un plan d'adressage IP. L'objectif de ce plan est d'une part de définir des règles d'adressage adaptées au contexte et d'autre part d'anticiper sur l'utilisation qui pourra être faite de la connexion au réseau Internet.

Cependant l'utilisation de plus en plus fréquente de protocoles d'affectation d'adresse IP dynamique (tel que DHCP) permet d'amoindrir l'effort de conception et surtout le travail d'adminstration d'un réseau IP.

Cette étape même si elle peut être simplifiée ne doit pas être négligée.

D'autre part, la recommandation RFC 1918 propose l'utilisation, pour les Intranets, de classes d'adresses particulières, non routables sur l'Internet.

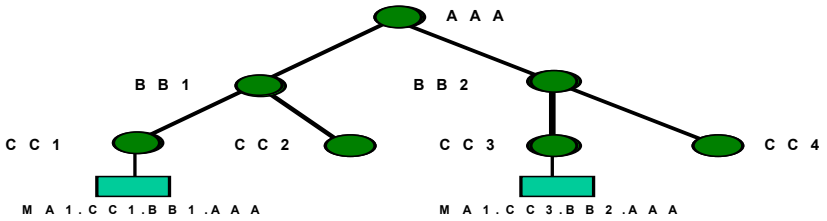
3.2. Le service DNS

3.2.1. Principes de DNS

Plus conviviaux à manipuler que des adresses IP, on a donné des noms à chacune des machines d'un réseau TCP/IP. Historiquement, chaque machine comprenait un fichier HOSTS qui effectuait la correspondance entre nom descriptif et adresse. Toutefois, avec la multiplication des machines sur l'Internet il n'était plus possible de tenir à jour des tables dans chaque machine.
Il a donc été spécifié le Domain Name System (DNS). Le DNS est une base de données distribuée, un certain nombre de machines (serveurs DNS) contrôlant des parties de la base, tandis que l'ensemble de celle-ci est accessible par un protocole de type Client/Serveur. Des mécanismes complémentaires permettent de fiabiliser la base (réplication) et d'augmenter les performances (caches).

Structure de nommage

Le nommage DNS s'appuie sur une organisation en arborescence définissant plusieurs niveaux de hiérarchisation, selon le modèle suivant :



Chaque ***noeud*** de l'arbre porte un label qui l'identifie par rapport à son ***parent*** (noeud de niveau supérieur). Chaque noeud peut avoir un ou plusieurs noeud ***fils*** (noeud de niveau inférieur). Au niveau mondial (Internet) le haut de l'arbre dispose d'un noeud racine, sans label, appelée « . » ou racine.

En dessous, un niveau de noeuds est normalisé :
com, edu, net, ..., principalement aux Etats-Unis,
jp (Japon), ca (Canada), fr (France), ... identifiant des zones géographiques.

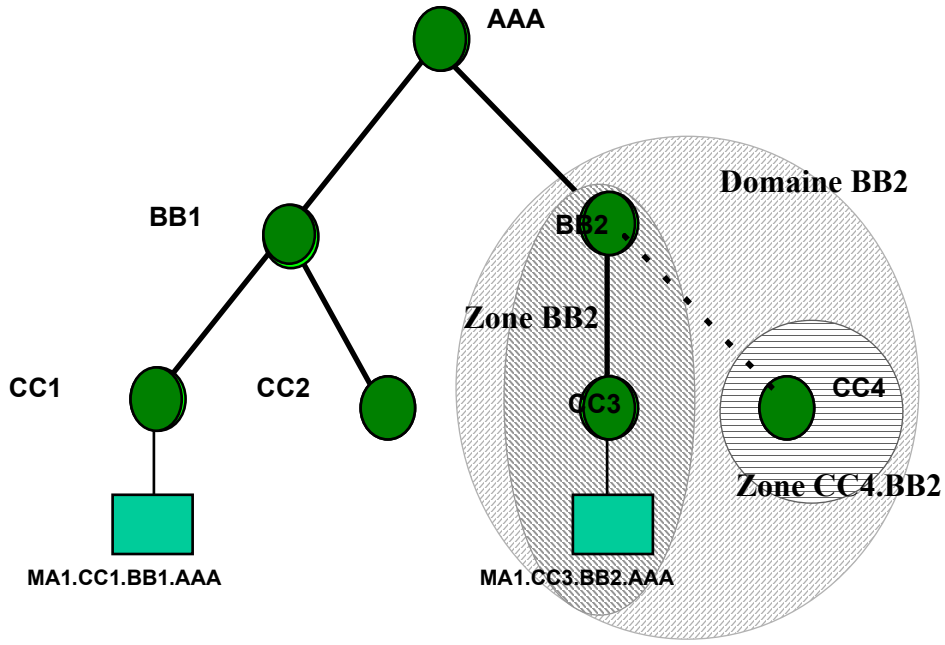
Le NIC (Network Information Center) gère les affectations des labels de noeuds fils de ces noeuds normalisés. En particulier, le NIC France gère le domaine FR.

Seuls sont autorisés, les lettres, les chiffres et le caractère « -« . Un label ne fait pas plus de 63 caractères (max de 12 conseillé) et un nom complet (Full Qualified Domain Name ***FQDN***) ne doit pas dépasser 256 caractères.

Un ***domaine*** représente toute la partie de l'arborescence qui se trouve sous un nom donné. Un ***sous domaine*** S d'un domaine D est la partie de l'arborescence à l'intérieur de D et à partir du noeud fils S.
Ex : BB1 est un domaine et CC2 est un sous domaine de BB1.

Du fait de sa structure distribuée, le service DNS d'un domaine peut être réparti sur plusieurs serveurs DNS. Pour cela on introduit la notion de ***zone***. Une zone est une partie de l'arborescence entièrement gérée par un serveur DNS.

Pour assurer la mécanique de répartition de la mise à jour on s'appuie sur le principe de ***délégation de zone***. Il est alors possible de définir des aires de responsabilité dans le nommage. Ainsi chaque branche reliant un noeud père à un noeud fils peut véhiculer une information indiquant qu'il délègue la responsabilité de nommage de niveau inférieur, lui même pouvant faire une délégation de zone avec ses niveaux inférieurs



Serveur DNS

Un serveur DNS possède une ou plusieurs zones de la base de données. Un serveur qui dispose de la version officielle des données d'une zone a ***autorité*** sur cette zone. Un serveur qui dispose des informations d'une zone, sur lequel il a autorité, dans un fichier de configuration est appelé ***serveur primaire*** pour cette zone. Un ***serveur*** est ***secondaire*** d'une zone lorsqu'il dispose des informations de cette zone par téléchargement à partir du primaire de cette zone (un mécanisme régulier de vérification de changement de zone est mis en œuvre entre le secondaire et le primaire). Il a alors lui aussi autorité sur cette zone.

Afin de limiter les temps de réponse, un serveur DNS stocke les informations qui passent par lui et qui ne concernent pas sa zone : c'est la fonction ***cache***. N'ayant pas autorité sur ces données, celles-ci contiennent une durée de validité définie par le serveur autoritaire de la zone.

Une zone ne peut avoir qu'un seul DNS primaire, éventuellement plusieurs secondaires.
Un serveur DNS peut gérer plusieurs zones étant pour chacune soit primaire soit secondaire.

En plus de l'adresse IP (A) du noeud recherché, les informations du DNS peuvent contenir un ensemble d'autres informations telles que le nom du serveur d'autorité du noeud (HINFO), le nom de la machine en charge du courrier pour ce domaine (MX).

Client DNS

Les clients DNS, appelés ***resolver***, soumettent des requêtes aux serveurs, en général toujours le même (le primaire de leur zone).
La fonctionnalité principale est la demande d'une adresse IP pour un nom donné.
La fonctionnalité inverse (adresse IP pour obtenir le(s) nom(s) existe aussi).
Une troisième fonctionnalité est très utilisée (messagerie). Elle permet de retourner, pour un nom de domaine (ce qui est derrière le @ d'une adresse Mail), quelle est la machine à laquelle il faut envoyer le courrier pour ce domaine (enregistrements MX).

Dialogue Client /Serveur

Deux types de dialogue entre le ***resolver*** et le(s) serveur(s) DNS.

Mode itératif : A la question du client, le serveur « de rattachement » renvoie une réponse indiquant qu'il ne peut résoudre l'adresse mais qu'il connaît un autre DNS susceptible d'avoir la réponse. Le client envoie la requête à ce deuxième serveur qui soit connaît la réponse soit indique un nouveau serveur mieux renseigné, ... etc.

Mode récursif : A la question du client, s'il ne peut résoudre, il fait suivre (***forwarder***) à un autre serveur qu'il pense être mieux renseigné, attend la réponse et la renvoie au client.

3.2.2. Plan de nommage DNS d'un Groupe

L'idée générale est de définir un domaine global Groupe, noeud père de noeuds englobant chacun un établissement du Groupe pour lesquels il délègue à chacun la responsabilité sur sa zone.

Règle : Plan de nommage DNS d'un Groupe

La structure d'un nom de machine est la suivante :

<Identification machine>(.<Ss domaine>).<Nom Etab>.<Domaine Groupe>.FR

<Domaine Groupe>

Ce nom va décrire, pour le monde entier (Internet) l'ensemble des noeuds du domaine.
A ce titre, il est déposé auprès du NIC France ou NIC.

Le nom de domaine Groupe est : **XX**

<Nom Etab>

Cette structure va permettre d'identifier des sous domaines, correspondant à chaque entité du Groupe (filiale, …) à l'intérieur du domaine. On va alors pouvoir définir des zones de responsabilité par établissement et ainsi éventuellement distribuer des serveurs DNS.
Les noms d'établissements sont les suivants : (reprise des noms établis pour le nommage X400) :

Etablissement.XX.fr

<Ss domaine>

Ce champ supplémentaire, facultatif et déconseillé (afin d'éviter des structures de nom trop longue), peut répondre à certains besoins d'un établissement qui souhaiterait disposer d'une granularité plus fine. Ex : identifier une filiale d'un établissement régional.

<Identification machine>

Ce dernier champ, qu'il serait souhaitable de limiter à 12 caractères maximum, identifie une machine IP dans son noeud.

3.3. Le service de messagerie (SMTP)

3.3.1. Principes de la messagerie SMTP

Simple Mail Transfer Protocol (RFC 821, 822 (structure entête) et 1651(commandes étendues)) est le protocole mis en œuvre sur l'Internet pour assurer l'échange électronique de messages.

C'est sans doute le premier service qui a contribué au succès d'Internet.

Il définit le mode de dialogue entre un client et un serveur pour l'envoi d'un message et entre deux serveurs SMTP pour le routage des messages.

La principale caractéristique de la messagerie est son fonctionnement asynchrone. En effet, l'émetteur d'un message et son destinataire n'ont pas besoin d'être connectés simultanément pour échanger des messages.
L'émetteur envoie son message à son serveur SMTP de rattachement en indiquant l'adresse du destinataire. Ensuite le serveur SMTP se charge de localiser le serveur SMTP destinataire et lui transfère le message (plus précisément au gestionnaire de boite à lettres).

Le logiciel du serveur de messagerie sauvegarde le message dans une boîte postale (Message Store), sur laquelle le destinataire viendra se connecter pour récupérer ses messages.
Pour récupérer son message, le destinataire interroge sa boite aux lettres. Pour cela, plusieurs protocoles ont été définis, tels que Post Office Protocol POP2, POP3 (RFC 1725) ou Internet Message Access Protocol IMAP4 (RFC 2060).

Le plus standard et le plus répandu aujourd'hui est **POP3**.

L'évolution se fait actuellement vers **IMAP4**, protocole similaire à POP3, mais auquel s'ajoutent des fonctionnalités, notamment celles de traitement de messagerie hors ligne et de re-synchronisation de boite.

SMTP, en tant que standard mondial de messagerie, permet d'assurer une compatibilité maximale entre les différentes messageries propriétaires. De plus, en tant que standard de l'Internet il assure l'échange de messages avec Internet.

Historiquement, la messagerie SMTP (issue du monde UNIX) ne transporte que des caractères ASCII 7 bits. Ce qui est déjà un inconvénient pour les messages simples - suppression des caractères accentués -, devient rédhibitoire si l'on souhaite échanger des pièces jointes telles que des documents structurés ou des fichiers multimedias, ce qui est possible au travers des « attachements ».
Des algorithmes de codage sont mis en œuvre dans les clients de messagerie de façon à véhiculer toute sorte d'information tels que UUENCODE ou BINHEX.

Le standard aujourd'hui est MIME - Multipurpose Internet Mail Extensions (RFC 1341 et 1342, révisées par les RFC 1521 et 1522).

Une évolution sécurisée S-MIME, permettant de chiffrer les pièces jointes au message, est de plus en plus répandue.

3.3.2. Structure des adresses eMail

Unification des adresses

La fédération des messageries implique une unification de la forme des adresses de courrier électronique. L'identité d'une boite aux lettres doit être divulguée sous une forme unique quel que soit l'établissement dans lequel se trouve l'utilisateur. De même qu'il est souhaitable que la forme des adresses soit la même, à l'intérieur de l'Intranet ou à l'extérieur, il est indispensable que les formes d'adresses soient identiques au sein du groupe. Ainsi tous les utilisateurs de groupe pourront transmettre une identité utilisable en n'importe quel point du réseau.
L'unification des adresses rendra possible l'utilisation d'un annuaire cohérent.

La structure générale d'une adresse eMail est la suivante :

<prenom.nom_utilisateur>@<nom de domaine>

<prénom.nom_utilisateur> est l'identifiant de l'utilisateur ou d'une liste

@ se prononce « at » un séparateur de champ (obligatoire)

<nom de domaine> est le nom du domaine qui possède le serveur pour la réception des messages SMTP de cet utilisateur.

Recommandation : pour être compatible sur Internet, les adresse eMail doivent être en minuscule et sans caractère accentué.

3.3.3. Prise en compte des messageries régionales

La topologie de l'infrastructure Intranet est en étoile, la communication entre deux établissements de la même région ne doit pas générer, dans la mesure du possible, de trafic sur le réseau Inter-Régional. Seule la communication entre les régions ou la communication avec Internet donne lieu à l'utilisation de la bande passante du réseau Inter-Régional.
Par contre, la passerelle vers l'Internet se situera en un seul point du réseau, en relation directe avec une zone de sécurité (voir chapitre sécurité).

L'administration des utilisateurs

L'administration des utilisateurs représente de loin le coût le plus important. Elle concerne des opérations récurrentes qui peuvent devenir très lourdes dès lors qu'elles sont centralisées. L'ajout et la suppression d'utilisateurs doivent être au maximum délégués vers les régions ou les établissements si c'est possible.

Annuaire de messagerie
Le Standard d'annuaire sur Internet est en passe de devnir le proctole : LDAP

Listes de diffusion
La mise au point de listes de diffusion demande une administration particulière. Elle ne concerne pas forcément que les utilisateurs de l'Intranet mais il doit être possible d'y inclure des adresses externes (clients,...).

3.3.3.1.Scénarios d'architecture d'interconnexion

L'interconnexion des messageries d'établissement sur l'infrastructure SMTP va se réaliser selon 2 cas :

- **L'établissement dispose d'une messagerie native SMTP**

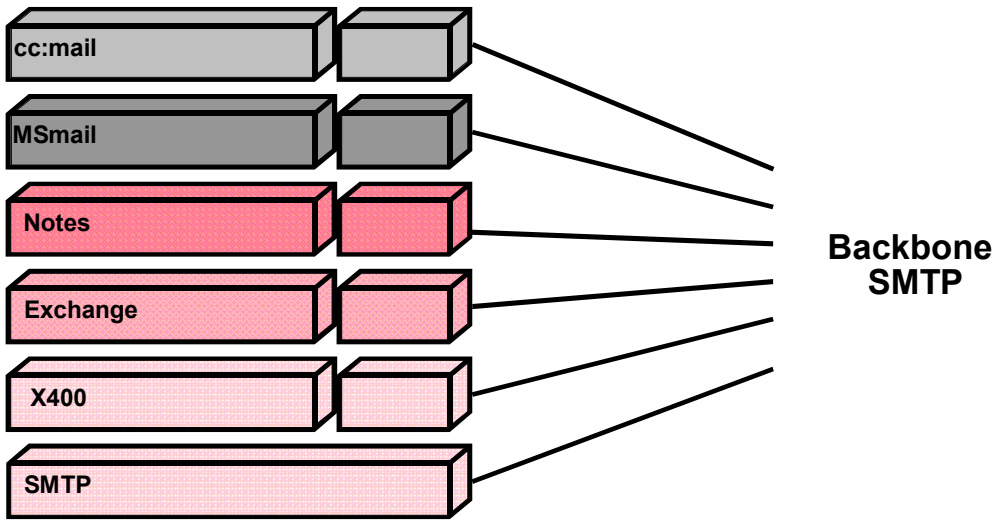
Sous réserve de mise à niveau des versions de logiciels, comme MIME, afin d'être cohérent par rapport à l'infrastructure fédératrice et des paramètres de configuration (DNS, entre autre), le raccordement se fait directement sur le point d'accès.

- **L'établissement dispose d'une messagerie non SMTP**

Dans ce cas de figure, l'interconnexion doit être effectuée selon les règles énoncées précédemment, donc au travers d'une passerelle d'adaptation entre les protocoles.

Règle : L'interconnexion des messageries propriétaires régionales sur le backbone fédérateur SMTP sera réalisée grâce à la mise en œuvre de logiciels passerelles fournis par les éditeurs de ces messageries propriétaires.

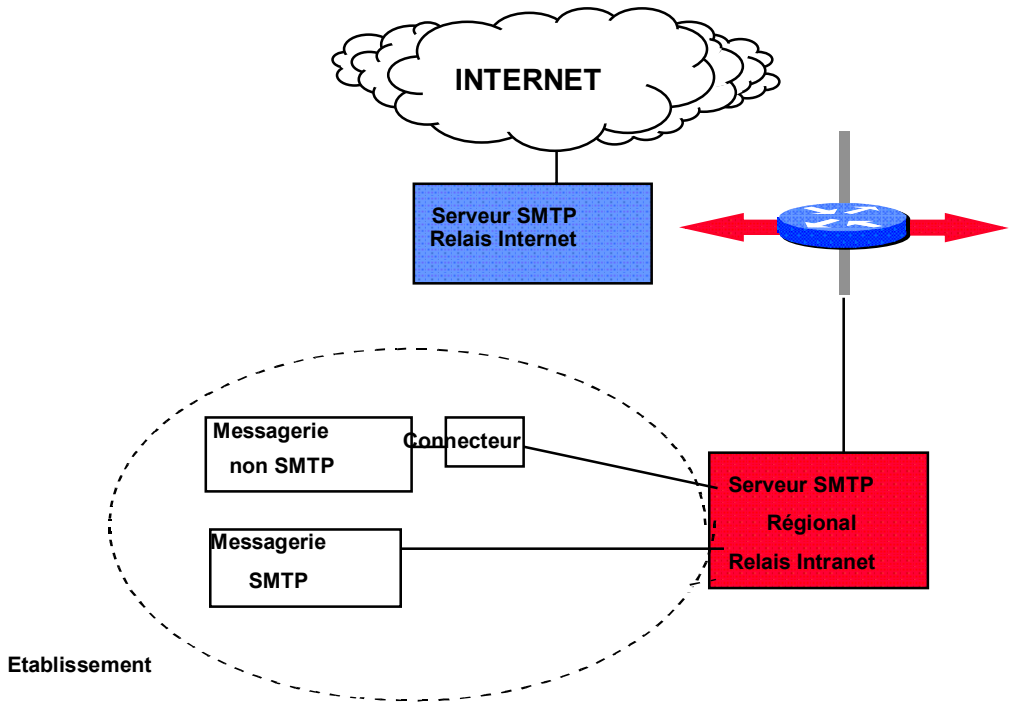
Cette approche consiste à équiper chaque messagerie propriétaire d'un « connecteur » SMTP et de réaliser un backbone SMTP de bout en bout. La plupart des messageries propriétaires, tels que MS/Mail, CC/MAIL, Notes disposent d'un tel composant étant donné le standard que représente SMTP. Toutefois, ces différents connecteurs ne sont pas forcément à un même niveau fonctionnel, ce qui peut entraîner des pertes d'informations.



3.3.4. Architecture de l'infrastructure de messagerie SMTP.

L'architecture proposée ci-dessous répond à la problématique d'échanges de messages entre les différents collaborateurs d'un Groupe d'une part, mais aussi l'échange de messages sécurisés entre les collaborateurs du Groupe et des interlocuteurs eMail sur Internet.
Elle tient compte également des contraintes de reprise de l'existant décrites ci-dessus.

Le schéma général est le suivant :



■ Routage des messages

Utilisateur Intranet vers utilisateur Intranet

Dans cas, le routage des messages est dirigé par le service DNS. C'est lui qui décrit la machine réceptrice du domaine de destination indiquée dans l'adresse eMail (enregistrement MX). Le routage est alors effectué au niveau IP.

Echanges avec Internet

Pour des raisons de sécurité (voir chapitre sécurité), il n'est pas souhaitable que chaque DNS Intranet dispose d'un accès à Internet. Il est alors nécessaire de transiter par un serveur relais, vers lequel seront routés tous les messages ayant comme destinataire toute personne hors du domaine.
Pour réaliser cette fonction il est nécessaire de passer par un routage applicatif, qui ne peut être réalisé par les DNS.

La plupart des serveurs SMTP savent gérer cette fonction d'envoi vers un serveur relais de tous les messages qui ne sont pas adressés à un domaine particulier.

■ Serveur SMTP principal- Relais Intranet

Le rôle du serveur national est essentiellement d'effectuer un relais entre l'Intranet et l'Internet. Il va concentrer tous les messages venant des utilisateurs de l'Intranet et destinés à l'Internet.
Grâce à un dialogue spécifique et contrôlé (via l'architecture de sécurité) il fournit ces messages au serveur principal - Relais Internet qui lui les envoie sur Internet.

■ Serveur SMTP principal- Relais Internet

Le rôle du relais principal est équivalent à celui du relais Intranet mais pour les messages à destination d'utilisateurs Intranet.
Il utilise le même dialogue sécurisé avec le relais Intranet pour transporter les messages venant de l'Internet vers l'Intranet.
Ce serveur réalise d'autres fonctions de contrôle des messages notamment sur les pièces jointes (voir partie sécurité).

■ Nommage des serveurs de messagerie

Le serveur de nom de domaine autoritaire pour le domaine <Nom Etab>.xx.fr va donner le nom du serveur pour la réception de messages SMTP.

Chaque serveur de messagerie répond à un ou à plusieurs domaines distincts. Un même domaine ne peut être géré que par deux serveurs différents.

Par convention, on nommera dans les DNS le serveur de messagerie pour le domaine <Nom Etab>.xx.fr par :

mail.<Nom Etab>.xx.fr

On ajoutera un deuxième nom pour ce serveur de messagerie :

pop.<Nom Etab>.xx.fr

mail sera utilisé pour toute les configurations SMTP (champs *MX* dans les DNS, champs *serveur SMTP* pour la configuration de clients...).
pop pour la configuration des clients (champ *serveur POP* ou *POP server*) (en cas d'utilisation de serveur POP).

Cela correspond à la configuration par défaut de la plupart des clients d'une part et permet d'autre part de garantir à long terme de pouvoir (notamment pour des raisons de charge) séparer ces deux fonctionnalités sur des machines différentes sans reconfigurer l'ensemble du parc de clients.

3.4. L'annuaire (LDAP)

3.4.1. Principe des annuaires

Un annuaire a pour objectif de devenir un référentiel dans lequel est stocké, non seulement les personnes, mais aussi les applications, les machines, etc. Il s'agit de consolider dans un référentiel unique, ce qui aujourd'hui est présent en de multiples endroits (serveurs de messagerie, serveurs de fichiers, applications, etc.).

Cet espace de nommage logique global des composants d'un Système d'Information sera intégré à celui-ci : des composants, applications ou services déclareront leur existence au travers de l'annuaire et d'autres composants, applications ou services trouveront les premiers grâce à l'annuaire.

L'ISO a spécifié une architecture et des protocoles définissant, de manière complète, un standard d'annuaire, sous la terminologie X500. Mais, la richesse de la spécification entraîne une lourdeur d'implémentation et le marché n'a pas encore suivi.

A plus court terme, et dans le cadre de l'Intranet, la problématique se limite (pour l'instant) à un annuaire des utilisateurs (notamment pour la messagerie). En effet, il n'existe pas à ce jour de solution standard de constitution d'un annuaire des utilisateurs Internet/Intranet, comme il existe des annuaires Exchange, Notes, ou la NDS de Novell.

Afin de résoudre ce problème, la communauté Internet s'est attachée à proposer une solution.

Première avancée, un protocole d'accès aux annuaires, Lightweight Directory Access Protocol (**LDAP**), inspiré du protocole DAP d'X500 de l'ISO, a été conçu pour être adapté à l'Internet.
Soutenu par les grands acteurs du marché, ce protocole a été accepté par l'IETF (RFC 1777, 1778, 1779). Il peut être considéré à ce jour comme un standard incontournable pour les applications accédant à un annuaire, et est implémenté (ou annoncé à court terme) sur les offres des éditeurs tels que Microsoft ou Netscape.

Règle : le protocole d'accès au service d'annuaire du Groupe sera donc réalisé grâce au protocole LDAP.

Néanmoins, la standardisation du protocole d'accès n'est qu'une première étape dans la réalisation d'une architecture d'annuaire global Internet. En effet, il reste à standardiser tout ce qui concerne le cœur de l'annuaire : le contenu de ces annuaires et les principes de réplication ou de synchronisation en cas d'annuaires répartis.

L'évolution autour de LDAP commence à apporter des réponses sur ces points en s'inspirant fortement de l'ISO X500, avec des leaders comme Netscape, et maintenant Microsoft, autour d'une spécification LDAP V3.

L'année 1998 devrait apporter des éléments de réponse significatifs sur ce sujet étant donné l'importance que prennent les annuaires dans une architecture Intranet.

■ Nommage des objets dans l'annuaire

La base LDAP est une base objet.

Le modèle des données : définit la syntaxe des données de la base

Le modèle organisationnel : définit la structure des informations dans l'annuaire, chaque structure est représentée par un noeud (DN). C'est une arborescence dont les premiers niveaux sont le pays, puis l'organisation, puis le nom de la ressource, etc.

Le modèle de sécurité : définit l'accès sécurisé aux informations de l'annuaire.

Le modèle fonctionnel : définit les opérations d'accès aux objets: ajout, suppression, modification, renommage et intérrogation.

Le modèle topologique : définit l'interopérabilité entre services d'annuaires interconnectés, permettant à ceux-ci de former un annuaire mondial.

Le nommage des objets de l'annuaire LDAP se conforme au standard X500, c'est à dire qu'il est structuré hiérarchiquement et du type champ=valeur, champ=valeur,...

Ce nom est appelé Distinguished Name (DN), il désigne sans ambiguïté un objet de l'annuaire.
Il est possible d'utiliser des champs pour rassembler des objets dans un sous-ensemble. On exploitera notamment cette possibilité pour :

- Définir des sous-ensembles géographiques
- différencier les éléments qui caractérisent des individus ou des ressouces.

Le jeu de caractères utilisable pour le nommage est uniquement ASCII, c'est à dire sans accentuation. Les espaces sont autorisés.

■ Les types d'entités manipulées par l'annuaire

- Les objets

Les objets de l'annuaire appartiennent tous à au moins une classe d'objets.
Une classe d'objets définit simplement un ensemble d'attributs obligatoires et un ensemble d'attributs optionnels. Un objet peut appartenir à plusieurs classes d'objets.

Il existe des classes d'objets 'standards', c'est à dire des classes décrites dans la recommandation X521, et des classes spécifiques qui étendent les premières.

Par exemple, les produits Netscape utilisent une classe spécifique *inetorgperson* pour décrire des objets personnes. Les besoins de l'annuaire d'une société nécessitent cependant souvent d'autres paramètres que ceux disponibles par défaut. Pour ces objets, on introduira donc de nouvelles classes d'objets spécifiques à l'entreprise.

- Les containers

Les containers sont des objets qui permettent de hiérarchiser l'annuaire. Tout objet appartient à une structure de container. Un container est un objet, à ce titre il dispose d'un certain nombre d'attributs.

3.5. La publication d'informations (HTTP)

Un serveur WEB est d'abord un serveur de documents, ces documents peuvent être des images, des pages Hypertexte, des sons, des vidéos, etc... .

Ce serveur utilise le protocole HTTP (HyperText Transfer Protocol).
Ce protocole est assez simple et aujourd'hui parfaitemement normalisé.

Le service HTTP n'entre que peu dans la complexité de la mise en place d'un intranet et c'est pourquoi ce chapitre n'est pas développé.

Bref rappel sur HTML :

HTML (HyperText Markup Language) est un langage permettant la conception de pages WEB.

Ce langage est constitué d'un jeu de commandes simples (tags ou balises) qui déterminent la structure du document, c'est à dire :

- les objets utilisés (tableaux, listes, textes, images, etc..)
- les couleurs
- les polices de caractères
- les liens hypertexte (voir ch précédent)

Exemple de codage HTML:

```
<HTML>
<TITLE>Ceci est un titre</TITLE>
<H2>Exemple</H2>
<BR>
</HTML>
```

Ce codage sera ensuite interprété par le navigateur qui fera le formatage et l'affichage du document suivant les capacités de la machine.

Ainsi, un document au format HTML est indépendant de la couche matérielle et peut être affiché sur n'importe quelle machine disposant d'un navigateur.

3.6. Le partage d'informations (NNTP)

3.6.1. Principes des groupes de news

Le principe de base est de créer un lieu de discussion commun pour un ensemble d'individus partageant un même sujet d'intérêt ou une même opinion. Tous les membres de ce groupe de discussion reçoivent tous les messages envoyés par les autres membres du groupe, et peuvent eux mêmes en rajouter. Il existe aujourd'hui plusieurs dizaines de milliers de groupe de discussion sur Internet (USENET), sur tous les sujets.

Le fonctionnement initial dérivait de la messagerie SMTP, suivant la RFC 822, les forums s'appuyant alors sur des serveurs de messagerie et des listes de diffusion.
Malgré plusieurs inconvénients, de nombreux groupes fonctionnent encore sur ce modèle, mais la majorité utilisent des serveurs de news communiquant grâce au protocole NNTP (Network News Transfer Protocol) (RFC 977), tout en conservant une structure de message proche de celle de la messagerie.

NNTP est responsable de l'acheminement des messages entre serveurs de news : gestion des forums existants, la recherche des nouveaux articles et leur diffusion d'un serveur à un autre. Il gère également les échanges entre le client et le serveur.
NNTP gère aussi un ensemble de messages particuliers permettant la gestion des listes de forums (création, suppression) (métainformations).

3.6.2. L'architecture du service de News

Le modèle réparti et coopératif du protocole NNTP permet de réaliser simplement une architecture de forums de discussion. De plus, l'implémentation de ce protocole sur Internet à grande échelle, avec des millions de messages échangés et des réplications périodiques, assure un fonctionnement correct.

Deux remarques s'imposent :

Les services de News peuvent se limiter à la mise en œuvre de forums de discussion uniquement Intranet.

La problématique organisationnelle, qui sort du champ de ce document, est un élément capital à prendre en compte pour assurer le succès d'un tel service :
création, suppression de groupe,
animation du groupe, modérateur,...

Par contre, la stabilité des spécifications NNTP depuis leur création n'impose pas de recommandation particulière que ce soit sur les serveurs ou sur les clients.

3.7. Le moteur de recherche

3.7.1. Principes du moteur de recherche

Les moteurs d'indexation sont issus de la rencontre de l'univers du Web et de celui de la GED (gestion électronique de documents). Cette double paternité est perceptible dans les fonctionnalités des produits, qui diffèrent en fonction de l'origine des logiciels :

- Web → Alta Vista, Microsoft Index Server, Infoseek, Excite…
- GED → Verity, Fulcrum....

Les premiers sont plus rustiques, mais plus simples d'utilisation et potentiellement plus puissants ; les seconds sont plus élaborés (ils utilisent les ressources de la linguistique), mais plus complexes à utiliser, et souvent plus onéreux.

Les principes de fonctionnement restent les mêmes. Une fois installé sur le serveur, le moteur indexe les fichiers en retenant leur adresse. Les fichiers concernés recouvrent divers types de format :

- les fichiers html bien sur, qui jouent un rôle central dans un Intranet
- les fichiers texte ASCII
- les fichiers texte, bureautique (Microsoft Office…)
- les fichiers de messageries (Mime, Lotus, MS Exchange…) avec un traitement particulier en fonction du logiciel choisi.

A une heure définie par l'administrateur, le moteur indexe les nouveaux documents. Cette opération consomme une grande partie des ressources systèmes, et peut mettre en péril le travail collaboratif. Elle doit donc être programmée à une heure de faible utilisation des ressources réseau. Le moteur doit par ailleurs être installé sur une machine suffisamment puissante, et fortement dotée en mémoire Ram (64 Mo dédiés minimum pour la plupart des produits). Plus la quantité de documents à indexer est importante, plus la tâche sera longue et consommatrice en ressources système. Enfin, l'opération d'indexation ne doit concerner que les nouveaux documents, ou les documents récemment modifiés.

Chez la plupart des éditeurs, les gammes proposées répondent à un tryptique :

- Une version " personnelle " (ou " worksation ") du logiciel, qui tourne sur le micro-ordinateur de l'utilisateur et indexe son seul disque dur.
- Une version " réseau local", qui indexe les serveurs reliés au réseau local, sans sortir de l'entreprise.
- Une version ouverte, qui indexe les serveurs reliés au Lan, ainsi que le web externe (Internet), selon des URL prédéfinis en fonction des centres d'intérêts des utilisateurs (naturellement il n'est pas question d'indexer l'ensemble du web).

La plupart des serveurs sont consultables et paramétrables à partir d'un navigateur standard. La recherche peut porter sur :

- un mot clef (procédés classique sur les annuaires et les " crawlers " du web)
- une question posée en " langage naturel " (c'est à dire une question en clair : quel temps fait-il à Paris ?). Un certain nombre de logiciels de recherche ne le permet pas.
- une requête en logique booléenne (and/or/not/near), entendez par là une requête sur plusieurs mots permettant d'affiner la recherche. A titre d'exemple, on peut demander au moteur de sélectionner les documents comprenant le mot " airbus" et le mot " boeing ". Cette recherche permettra de trouver des articles parlant des deux constructeurs. A l'inverse, on peut demander une recherche portant sur le nom " mazda ", mais excluant les mots " car ", " voiture " et " japan " pour ne cibler que les documents portant sur le fabriquant de piles électriques.

Les moteurs d'indexation sont souvent multilingues. Cette notion de multilinguisme n'a pas le même sens selon les produits. Ainsi, un moteur comme Alta Vista permet à l'utilisateur de choisir la langue des documents trouvés sur une requête particulière : l'utilisateur peut demander au moteur de n'afficher que les seuls documents en langue française.
Un moteur plus perfectionné, utilisant les ressources de la linguistique, intègre la logique de la langue pour affiner la recherche ; il proposera un choix de langues plus réduit, mais exploitera plus à fond la logique propre à chaque idiome.

Enfin, chaque produit propose ses spécificités, destinées à différencier l'offre de la concurrence.
Ainsi, la fonction " refine " d'Alta Vista permet à l'utilisateur d'exclure les réponses proposées par le moteur lorsqu'elles s'éloignent de la réponse souhaitée. Le moteur intègre les occurrences que l'utilisateur a exclu, et renvoie une sélection affinée, théoriquement plus conforme aux attentes de l'utilisateur. il peut également proposer un graphique (mapping) de proximité sémantique. Malheureusement, parce qu'elle repose sur des principes purement statistiques, cette fonction donne des résultats peu satisfaisants.

Autre fonction, la détermination du rang de présentation des réponses en fonction des " occurrences ", c'est à dire de la proximité avec la question posée. Ici aussi, la pertinence du résultat dépend de la méthode employée par le moteur. Utilisant une démarche uniquement statistique, Alta Vista compte le nombre de fois où le mot apparaît, alors que Verity cherche des proximités sémantiques avec la question posée.

3.8. La sécurité d'interconnexion Internet

3.8.1. Problèmatique de sécurité sur Internet

Le réseau Internet est constitué de l'interconnexion de très nombreux réseaux, mis en oeuvre et administrés par des entités distinctes réparties sur l'ensemble du globe : organismes scientifiques et éducatifs, militaires ou commerciaux. Par accès à l'Internet, on entend en réalité :

- la capacité d'accéder via Internet aux très nombreux autres sites qui disposent d'une connexion sur Internet,
- la mise à disposition de ressources à tout ou partie des utilisateurs de ces différents sites.

Ces deux aspects posent des problèmes de sécurité, qui vont être détaillés dans cette partie de l'étude.

3.8.1.1.DNS

- Le DNS peut être attaqué par pollution de ses tables.
- Certaines faiblesses d'implémentation permettent l'interposition de machines au moment de la résolution d'adresse.
- Il permet également d'obtenir des informations sur le parc géré.

3.8.1.2.Mail

- Le protocole SMTP ne permet pas d'authentifier l'origine des messages.
- L'outil utilisé comme serveur SMTP sous UNIX, *sendmail,* présente de grands dangers (il fonctionne souvent en mode *root*) et comporte des bugs de sécurité (permet d'exécuter des commandes sous *root*).
- La messagerie peut faire office de vecteur pour des virus, des vers, des chevaux de Troie et des bombes logicielles.
- Aucune confidentialité n'est assurée, et il n'y a pas d'assurance de remise des messages.
- Par ses commandes VRFY (verify) et EXPN (expand), un serveur SMTP peut faciliter l'identification des comptes déclarés et d'accès à des traitements automatisés de messages.

3.8.1.3.WWW

- Les réponses aux requêtes peuvent inclure des programmes à lancer pour traiter la réponse : ceux-ci nécessitent d'être contrôlés.
- Les mécanismes d'authentification, lorsqu'ils sont employés, sont généralement faibles.
- Les contrôles des demandes de transfert de fichiers ne sont pas toujours suffisants et créent une faille sur le serveur en permettant parfois d'outrepasser les permissions en place.
- Le partage de l'arborescence avec un serveur FTP Anonyme peut permettre de déposer des fichiers à faire interpréter par la requête.
- Les requêtes permettent de déclencher l'exécution de scripts CGI. Ces scripts doivent donc être très contrôlés pour éviter des effets de bords désastreux.
- Les programmes Javascript, les applets Java, et les contrôles ActiveX peuvent être dangereux malgré les contrôles théoriquement imposés par les langages. Ils peuvent être utilisés pour établir des connexions réseau, lire, modifier ou effacer des fichiers, interagir avec d'autres applications. On constate actuellement une importante prolifération de scripts et d'applets hostiles, certaines sources pouvant même être consultées.

3.8.1.4.News

- Les risques encourus lors de l'utilisation des News sont similaires à ceux qui existent pour la messagerie.

3.8.1.5.FTP

- L'authentification requise par le protocole fait circuler en clair le nom du compte utilisé et le mot de passe correspondant.
- La présence de permissions insuffisamment strictes sur des fichiers et des répertoires rend possible le remplacement ou la création de fichiers par FTP.
- Des fichiers de configuration de la machine comme /etc/passwd et /etc/hosts peuvent être rapatriés par FTP.
- Dans le cas d'un accès anonyme, les fichiers systèmes accessibles dans l'arborescence restreinte ne sont que des copies. Leur contenu peut toutefois fournir de l'information sur la machine (comptes et groupes existants).

3.8.1.6.Telnet

- Le mot de passe utilisé est véhiculé en clair sur le réseau.
- Des cas de compromission de *telnet* pour tracer mots de passe et nom du compte ou toute la session (cheval de Troie) ont été recensés.

3.8.1.7.Administration de réseau par SNMP

- L'altération des routes configurées sur les routeurs ou sur des machines terminales, possible par SNMP, permet d'engendrer un déni de service et porter atteinte à la confidentialité des informations.
- La désactivation d'une interface peut entraîner une indisponibilité plus ou moins grande d'un réseau.
- L'usurpation d'adresse IP peut être facilitée lorsque SNMP est utilisé sur la machine que l'on désire usurper (il suffit de changer son adresse).
- La modification de filtres permet de passer outre une politique de sécurité.

3.8.1.8.Autres protocoles utilisés sur Internet

- Le protocole IP n'est pas sécurisé. Même si des champs optionnels de sécurité existent, les implémentations courantes du protocole ne les utilisent pas.
- L'usurpation d'adresse IP est une des attaques les plus courantes du protocole IP. Une adresse IP est très facile à usurper, permettant de laisser supposer que l'on provient d'un site de confiance, ou même parfois du réseau interne.
- Le fonctionnement normal d'IP peut être détourné pour rediriger des paquets vers une machine pirate en utilisant les options de « strict source routing » et de « loose source routing » qui permettent de faire utiliser le chemin précisé dans la trame, même s'il n'est pas cohérent.
- Les connexions TCP peuvent être attaquées par détermination du sequence number à venir.
- Un pirate peut, par recalcul des cheksums et TCP sequence number de l'échange en cours, usurper une connexion en cours. Même une authentification très forte en début de session, ne permet pas de garantir qu'il n'y a pas intrusion pendant la session. La seule possibilité de garantir l'authentification dans la durée est de chiffrer ou au moins de signer les données échangées.
- Le protocole UDP est encore plus facile à attaquer. Il n'utilise en effet ni acquittement, ni séquencement des trames.
- UDP est par ailleurs un protocole non connecté. Tous les mécanismes d'authentification lors de l'initialisation de la connexion sont inefficaces pour le sécuriser. C'est pourquoi, ce protocole et tous les services qui l'utilisent sont à employer avec la plus grande prudence, et de préférence à éviter.
- ICMP (Internet Control Message Protocol), protocole de contrôle d'Internet, est utilisé par des pirates pour réaliser du déni de service (interrompre des connexions en cours en envoyant des messages de type « destination unreachable ») ou, plus gravement encore, pour rediriger du trafic vers leur station (à l'aide des messages « redirect route »).
- RIP (Routing Information Protocol) est utilisé pour déterminer le routage. L'émission de faux paquets RIP peut être utilisée pour rediriger des paquets vers une machine pirate, les routeurs faisant généralement peu de vérifications.
- Les mécanismes d'authentification des autres protocoles de routage d'Internet : OSPF et RIPV2 ne sont pas suffisamment puissants pour se protéger totalement du problème.

3.8.2. Mécanismes de sécurité sur les principaux services Internet

3.8.2.1.Mécanismes communs à tous les services

Authentification

- Il n'existe pas de mécanisme d'authentification commun à tous les services. Cependant, les mécanismes basés sur SSL (Security Socket Layer) s'étendent à de nombreux services.

Disponibilité

- Tous les mécanismes participant à protéger les données contenues sur le serveur (intégrité) et à empêcher l'intrusion (authentification, autres mécanismes) vont favoriser la disponibilité du serveur.
- Il reste néanmoins difficile de combattre une saturation du serveur par l'émission de nombreuses requêtes depuis un autre site.
- C'est pourquoi, il est préférable de cloisonner les serveurs en séparant les serveurs contenant des données à accès restreint pour des utilisateurs de sites connus, des serveurs contenant des données publiques. Des mécanismes de filtrage pourraient ensuite être mis en oeuvre pour éviter les requêtes provenant de sites indésirables.
- L'autre moyen pour augmenter la disponibilité des serveurs est de désactiver tous les services non utilisés.
- Enfin, l'utilisation de serveurs à système d'exploitation peu connu (comme Windows 3.1x, 95, NT) de préférence à Unix permet de rendre inefficace certains outils de piratage et certaines failles, notoirement connus. Ceci n'est cependant que transitoire, compte tenu de la diffusion de NT, son niveau de connaissance rejoindra sûrement Unix.

Intégrité

- L'intégrité des données présentes sur les serveurs peut être assurée en mettant en place une bonne gestion des systèmes de protection de fichiers des serveurs Unix ou NT utilisés.
  En effet, si chaque service utilise des espaces disques séparés, si les droits d'écriture sont strictement limités à des personnes authentifiées et habilitées, le risque d'altération des données est considérablement réduit.

Confidentialité

- La confidentialité des données est elle-même renforcée par la mise en place des mécanismes assurant la disponibilité et l'intégrité.
- Pour la confidentialité des échanges, certains standards émergeant comme SSL permettent d'améliorer la situation.
  D'autre part, pour des échanges entre des sites connus, il est possible d'utiliser des boîtiers externes de chiffrement, sous réserve d'obtention de l'autorisation des autorités (en France le SCSSI).

Autres

- Les logiciels serveurs, de même que les logiciels clients, sont des logiciels complexes, donc souvent buggés. Les bugs se traduisent souvent par des trous de sécurité. Une fois détectés, ces bugs sont rapidement corrigés par les fournisseurs. Il est donc important de toujours faire tourner les versions les plus récentes des logiciels.
- Bien sûr, la sécurité de tous les services Internet est renforcée par la mise en place des mécanismes de filtrage et de contrôle des firewalls.

3.8.2.2.Le Web

Authentification

- Des mécanismes permettant d'assurer l'authentification mutuelle entre le client et le serveur sont disponibles (Netscape, NCSA, ...).
- Ces mécanismes s'appuient sur la cryptographie à clés asymétriques, avec publication de certificat à une tierce partie (dit tier de confiance).
- Ces mécanismes permettent ensuite d'utiliser les mécanismes classiques de cryptographie à clés symétriques pour signer ou chiffrer les échanges entre le client et le serveur.
- Ces mécanismes permettent d'authentifier un utilisateur pour l'accès à certaines parties du serveur.

Disponibilité

- Les mesures générales s'appliquent ici.
- Le serveur Web ne doit pas s'exécuter avec des privilèges trop élevés. En cas d'intrusion sur le serveur, si le processus attaqué a des privilèges, le pirate pourra les utiliser pour détruire le serveur.

Intégrité

- Les scripts CGI (Common Gateway Interface) utilisés par les serveurs Web ne doivent pas être accessibles en écriture.
- Les scripts CGI doivent être écrits avec précaution afin d'éviter toute faille pendant leur exécution, notamment les failles permettant de prendre la main sur le système.
- Il est intéressant de signer les pages HTML et les scripts CGI afin de s'assurer que leur contenu n'a pas été modifié.

Confidentialité

- Les mécanismes SSL, SHTTP, SET permettent de chiffrer les échanges de données entre client et serveur.
- Appliquer aussi les mécanismes généraux.

3.8.2.3.Le transfert de fichier

Authentification

- Le transfert de fichier FTP permet plusieurs types d'authentifications. L'authentification basique de FTP n'est pas suffisante car le mot de passe circule en clair.
- Des authentifications basées sur des mots de passe non rejouables ou utilisant calculette ou carte à puce peuvent être utilisées, grâce à la mise en place des firewalls.
- Il faut cependant indiqué que les accès FTP anonymes ne sont pas authentifiés.

Disponibilité

- Les principes généraux s'appliquent, notamment la séparation des serveurs en fonction de la sensibilité des informations transmises.

Intégrité

- Des mécanismes de signature des données échangées de type PGP (Pretty Good Privacy) peuvent être utilisés pour contrôler l'intégrité des données échangées. Pour cela, il faut récupérer un PGP sur un serveur non-américain, il peut s'utiliser en signature sous réserve d'autorisation.
- Appliquer les principes généraux pour l'intégrité des données stockées.

Confidentialité

- Appliquer les principes généraux et/ou PGP sous réserve d'autorisation.

Autres

- Avec la messagerie, FTP est un des principaux moyens d'introduction de virus. Construire un sas de décontamination permettant de contrôler les fichiers reçus. Malheureusement, il n'existe pas de logiciel anti-virus intégré à FTP.

3.8.2.4.La messagerie

Authentification

- La messagerie SMTP ne fournit pas de mécanisme d'authentification.
- Pour authentifier l'origine d'un message, on peut recourir à l'usage de logiciels comme PGP (voir FTP).

Disponibilité

- Eviter l'utilisation du logiciel sendmail, et à défaut, toujours utiliser la version la plus à jour.
- Appliquer les principes généraux.

Intégrité

- La messagerie et ses dérivés (MIME) permettent de nombreux traitements automatisés des messages reçus. Il convient cependant de filtrer les messages reçus afin d'éviter l'introduction de virus et autres chevaux de Troie. Faire particulièrement attention aux macros incluses dans les fichiers issus de traitement de texte.
- Appliquer les principes généraux et/ou PGP sous réserve d'autorisation.

Confidentialité

- Appliquer les principes généraux et/ou PGP sous réserve d'autorisation.

3.8.2.5.Les forums - News

Authentification

- Les principes d'authentification de SSL devraient bientôt être disponibles pour les News.

Disponibilité

- Appliquer les principes généraux et ceux de la messagerie.

Intégrité

- Appliquer les principes généraux et ceux de la messagerie.

Confidentialité

- Appliquer les principes généraux et ceux de la messagerie.

3.8.3. Concepts de Firewalls

3.8.3.1.Définitions

Un Firewall peut être défini comme un ensemble de composants mis en œuvre entre deux réseaux, et contribuant à fournir les propriétés suivantes :

1. Tout trafic de l'intérieur vers l'extérieur ou de l'extérieur vers l'intérieur doit impérativement passer par le Firewall.
2. Seuls les flux autorisés conformément à la politique de sécurité peuvent franchir le Firewall.
3. Le Firewall est lui-même inaccessible, et de ce fait insensible aux attaques.

A ces trois propriétés de base s'ajoute une fonctionnalité importante, qui contribue notamment à différencier les Firewalls de simples routeurs sur lesquels on met en place des filtres : la génération de traces relatives à toute tentative de violation de la politique de sécurité, mais aussi aux communications autorisées.
Quelques termes se rencontrent fréquemment dès que le sujet des Firewalls est abordé dans le détail. Les plus importants sont définis dans ce paragraphe.

■ Bastion

Ce terme est employé pour désigner une machine exposée aux attaques en provenance de l'Internet ; elle bénéficie en général d'une configuration renforcée sur le plan de la sécurité (limitation des comptes et des services disponibles) lui permettant d'être immunisée contre les attaques qui peuvent être lancées contre lui.

■ Zone démilitarisée (DMZ)

Un réseau qualifié de zone démilitarisée possède en général les caractéristiques suivantes :

- Il est isolé du réseau privé protégé par le Firewall.
- Il supporte les machines vers lesquelles les utilisateurs d'Internet ont le droit d'établir des connexions (serveurs SMTP, Web, FTP, etc).
- Son accès depuis l'extérieur est contrôlé par le Firewall, mais avec une politique de sécurité moins drastique que pour le réseau interne.

La terminologie de « réseau bastion » est également employée pour désigner ce type de réseau.

3.8.3.2.Modes de contrôle

Bien que la plupart des Firewalls du marché utilisent une dénomination propre pour définir leur mode de fonctionnement, il est possible de définir plusieurs classes de produits.
On remarquera que certains Firewalls sont susceptibles d'appliquer plusieurs de ces méthodes. Il importe toutefois de savoir que pour un flux donné, une seule sera appliquée.

3.8.3.2.1.Contrôle au niveau des couches réseau

Filtrage de paquets (Packet Filtering)
Chaque trame subit une comparaison de certains de ses champs (adresses source et destination, numéros de ports source et destination, options protocolaires) avec les paramètres des filtres qui sont définis.
La notion de session n'est pas gérée.
Le filtrage d'éléments de niveau applicatif ne peut être envisagé que par comparaison de séquences de bits à des emplacements fixes dans les trames.
Ce filtrage constituant un mécanisme de très bas niveau, il peut être extrêmement rapide.
Ce bas niveau ne permet cependant pas d'avoir beaucoup de recul sur les flux. On notera en particulier que la gestion de la fragmentation IP est délicate, surtout lorsque le séquencement des trames n'est pas respecté, ce qui peut conduire à laisser passer des trames et donne donc prise à une saturation volontaire de l'accès protégé par le filtre de paquets.
Le principal désavantage de ce type de firewall, est qu'il ne dispose d'aucun mécanisme d'authentification s'il ne fait pas appel à d'autres mécanismes, comme par exemple une authentification sur une connexion établie en parallèle.
Relayage de circuits (Circuit Level Gateway)
Plus sophistiqué que le filtrage de paquets, ce mode de gestion gère la notion de connexion. Lorsqu'une connexion peut être établie conformément à la politique de sécurité, un contexte est créé en mémoire. Il sera détruit à la fin de la connexion. Tous les paquets d'un même flux sont rattachés au contexte correspondant et sont transmis au lieu d'appliquer les règles de filtrage à chaque paquet comme précédemment.
La notion de contexte permet une plus grande précision dans la gestion des flux : il est notamment possible de conditionner l'établissement d'une connexion de données FTP à l'existence d'un contexte pour la connexion de contrôle associée.
Pour les services basés sur UDP, qui fonctionnent en mode non connecté, la notion de session est gérée au moyen d'un compteur de temps.

3.8.3.2.2.Contrôle au niveau applicatif

Relayage applicatif (Application Level Gateway)
Chaque service réseau est géré par un programme spécifique (fréquemment nommé proxy). Ce programme sait en analyser le flux applicatif, et permet donc une plus grande finesse dans le contrôle offert, tant sur le plan du filtrage que de la traçabilité.
Un programme de relayage générique peut être utilisé pour tous les services ne disposant pas d'un programme spécifique (on ne bénéficie alors d'aucune fonction d'analyse du contenu du flux).
On notera que la mise en œuvre du relayage applicatif conduit à masquer les adresses des machines clientes. Il y a en effet deux connexions, la première initiée par le client vers le relais sur le Firewall, et la seconde initiée par le relais vers la machine de destination. Cette dernière voit donc une connexion provenant de l'adresse externe du Firewall.

Filtrage adaptatif (Stateful Inspection)

Il s'agit du mécanisme le plus récemment développé. Bien qu'agissant au niveau des trames, un contrôle des informations de niveau applicatif est réalisé. La finesse de contrôle est en général moindre que celle qui peut être obtenue grâce à un relais applicatif. Le niveau de performance qu'il est possible d'atteindre est par contre potentiellement plus élevé, du fait que le traitement est effectué sans que les données aient eu à remonter jusqu'au niveau des couches applicatives, auquel sont placés les proxy.

3.8.3.2.3.Contrôle du contenu

Un degré très avancé de contrôle de l'utilisation des applicatifs est atteint par certains des produits mettant en œuvre les deux modes de contrôle qui précèdent. Ils ont ainsi la capacité par exemple :

- De filtrer les commandes GET ou PUT du protocole FTP ou HTTP.
- De remplacer les informations relatives aux machines du réseau privé dans l'entête des messages électroniques.
- D'inhiber sélectivement les scripts ActiveX et javascript, ou les applets Java dans des flux HTTP.

Plusieurs raisons de contrôler le contenu des objets transmis au travers du Firewall peuvent être envisagées :

- Un contrôle antivirus appliqué de façon centralisée au niveau du Firewall aux messages et aux fichiers entrants offre une garantie de l'innocuité de toutes les informations qui arrivent par ce biais.
- Un contrôle antivirus appliqué aux messages et aux fichiers sortants peut être nécessaire pour préserver une bonne image de marque de la société.
- Une vérification de la nature du contenu des informations sortantes (sujet, mots-clés) peut être indispensable dans des contextes sensibles.

Les mécanismes nécessaires pour procéder à des contrôles de contenu peuvent être fournis par certains Firewalls, ou par des produits tiers.

3.8.4. Architectures d'interconnexion sécurisée

3.8.4.1.Contraintes d'adressage

Le plan d'adressage en usage sur le réseau interne de l'entreprise peut influer fortement sur l'architecture d'interconnexion.
En environnement TCP/IP comme avec les autres protocoles, il est indispensable que chaque machine bénéficie d'une adresse unique. A cette fin, les adresses IP d'Internet ont de longue date été attribuées par une autorité internationale.
De nombreuses sociétés, qui n'avaient jamais envisagé d'être reliées à l'Internet, sont désormais désireuses de se connecter à l'Internet que ce soit pour offrir des services ou pour bénéficier des services existants.
Il résulte de tout ceci des plans d'adressage incompatibles avec l'Internet :

- Soit parce que leurs adresses sont attribuées en tout ou en partie à d'autres entreprises ou organismes, si bien que l'interconnexion ferait coexister des machines dotées des mêmes adresses.
- Soit parce qu'elles utilisent certaines des adresses qui ne sont pas routées sur l'Internet.

Deux mécanismes permettent de limiter les problèmes d'adressage.

L'utilisation du protocole DHCP permet entre autres fonctionnalités l'attribution dynamique d'adresses IP. Par ce mécanisme, il est possible de réduire le nombre d'adresses en usage à un instant donné au seul nombre de machines ayant besoin de communiquer simultanément en TCP/IP. Cette solution n'est dans la pratique pas aisée à mettre en œuvre en raison de l'augmentation croissante de la part des protocoles TCP/IP sur les réseaux d'entreprise et de la généralisation de la supervision et de l'administration de réseau, qui s'appuie le plus fréquemment sur SNMP, lui-même supporté par IP.
Il s'avère que la mise en œuvre de DHCP sera dans beaucoup de cas principalement motivée par la facilité d'administration qu'elle permet, en permettant un stockage centralisé des informations de configuration réseau de toutes les machines.

La notion de translation d'adresses développée dans le paragraphe suivant apporte quant à elle une solution aux problèmes d'incompatibilité de plans d'adressage.

3.8.4.2.Translation d'adresses

Principe

Le principe de la translation d'adresses est le suivant : lorsqu'une trame IP est émise par une machine d'un réseau vers une machine d'un second réseau au plan d'adressage incompatible avec le premier, il est impératif que les adresses IP source et destination soient toutes deux compatibles avec le plan d'adressage du réseau qui transporte la trame.
Le mécanisme de translation doit être mis en œuvre à la frontière entre les deux réseaux, pour que les seules adresses apparaissant sur l'un et l'autre réseau soient en conformité avec les plans d'adressage locaux et les règles de routage en vigueur.

Caractère statique ou dynamique des translations

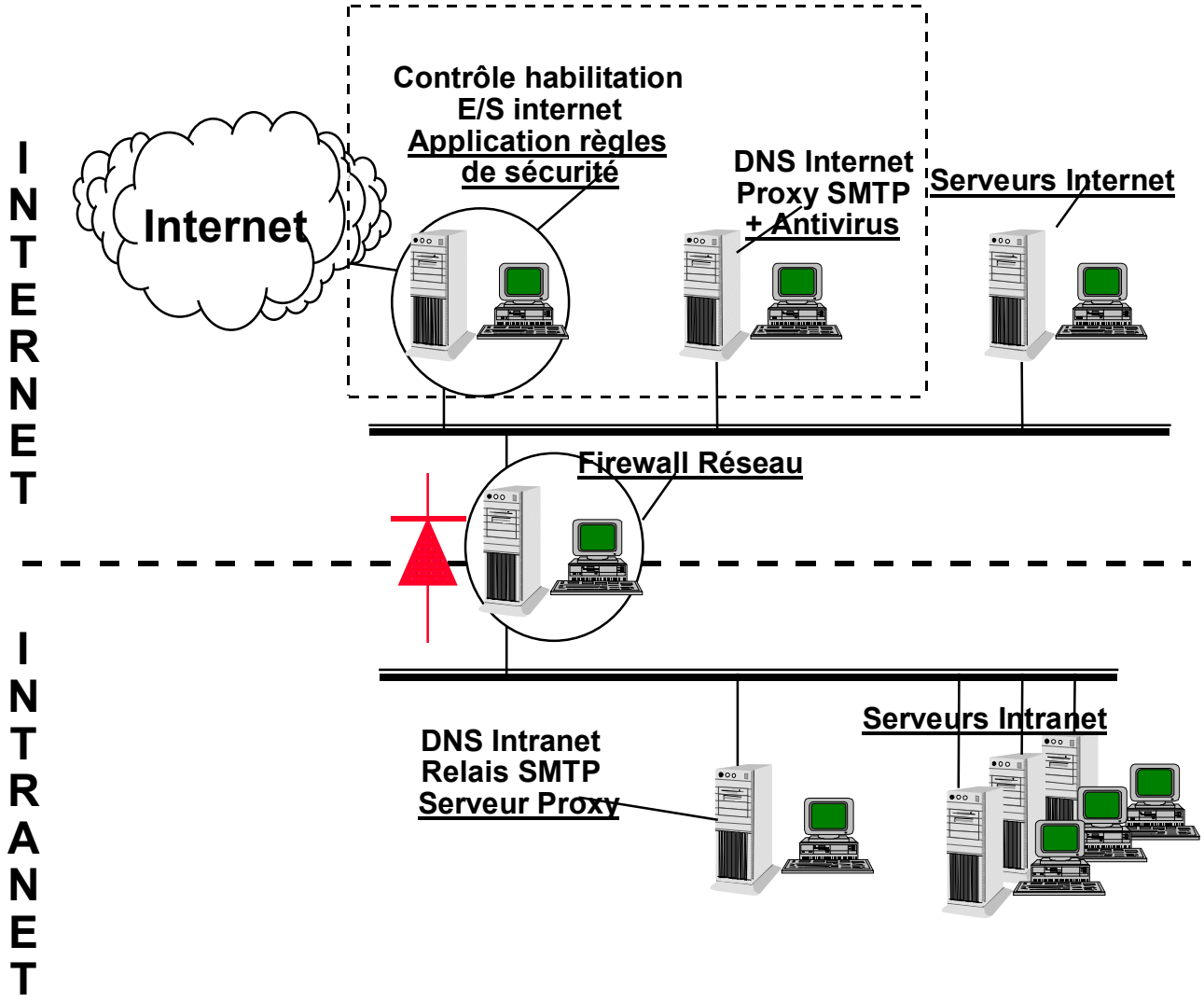
L'adresse officielle utilisée pour les communications d'une machine particulière du réseau privée peut être toujours la même, ou changer à chaque communication. On parlera dans le premier cas d'une translation statique, et dans le second d'une translation dynamique.
On choisira de mettre en œuvre des translations d'adresses statiques pour les serveurs qui doivent pouvoir être accédés depuis l'Internet, et des translations dynamiques pour toutes les machines qui sont exclusivement clientes de services offerts par d'autres machines de l'Internet.

Le masquage d'adresses

Le masquage d'adresses est une méthode essentiellement mise en œuvre par les programmes proxy sur un Firewall applicatif. Le mode de fonctionnement natif de ces Firewalls implique qu'une première connexion soit réalisée sur l'une des interfaces du Firewall, qu'une seconde soit réalisée depuis le Firewall vers la destination, et que le flux soit transmis de l'une à l'autre par le proxy .
La seconde connexion étant initiée par le Firewall, c'est son adresse qui apparaît comme adresse source de la communication. Il y a de ce fait un masquage total de l'adresse IP de la machine véritablement à l'origine de la communication. Cette même adresse est utilisée pour toutes les communications sortantes (en faisant varier dynamiquement le numéro du port source).

3.8.5. Architecture de sécurité d'interconnexion Internet

Le schéma ci-dessous présente l'architecture de sécurisation de l'Intranet vis à vis d'Internet.



L'infrastructure Intranet bénéficie de la sécurisation des deux niveaux de Firewall. Les accès entre l'Infrastructure Intranet et la DMZ n'ont aucun impact sur la configuration du Firewall Internet, qui bénéficie ainsi d'une configuration plus stricte que dans les cas précédents.

Remarques :
L'utilisation de deux technologies différentes pour les Firewall pourra représenter un niveau de sécurité supplémentaire.

Suivant les contraintes (services, performances, ...), l'environnement Firewall présenté ci-dessus pourra s'implémenter sur une ou plusieurs machines.

