Chapitre 8
Configuration des composants de transport

1. Présentation des services de transport

1.1 Principe de fonctionnement des services de transport Exchange

Comme indiqué dans les précédents chapitres, Exchange Server 2013 rompt avec les architectures des versions antérieures du produit. L'intégration des fonctionnalités de transport bénéficie des mêmes avantages que pour les rôles **Accès clients (CAS)** et **Boîtes aux lettres (MBX)** et, même si le rôle **Hub-transport** n'est plus directement exposé, il n'en demeure pas moins que le paramétrage et le fonctionnement interne restent très proches des précédentes versions.

Ainsi, les composants de transport ont pour objectif l'acheminement des messages aussi bien à l'intérieur qu'à l'extérieur de l'organisation Exchange, par l'intermédiaire de différents mécanismes de routage.

Le service frontal de transport hébergé par les serveurs d'accès client (CAS) agit comme un proxy SMTP sur le trafic entrant et sortant de l'organisation Exchange 2013. Aucune analyse du contenu n'est réalisée par celui-ci et il transmet directement les messages au service de transport d'un serveur de boîtes aux lettres (MBX) en bonne santé.

La sélection du serveur de boîtes aux lettres se fait sans prendre en compte ni le nombre, ni le type, ni l'emplacement des destinataires du ou des messages.

Le routage des messages peut se faire ensuite entre les différents services de transport hébergés par les serveurs de boîte aux lettres de l'organisation.

La segmentation des zones permettant le routage des messages se fait par des groupes de remise qui permettent de faciliter l'acheminement des messages afin d'améliorer l'efficacité des échanges au sein de l'infrastructure. Un groupe de remise peut-être : un groupe de disponibilité de base de données, un groupe de remise de boîtes aux lettres, un connecteur de serveur source, un serveur d'expansion de groupe de distribution…

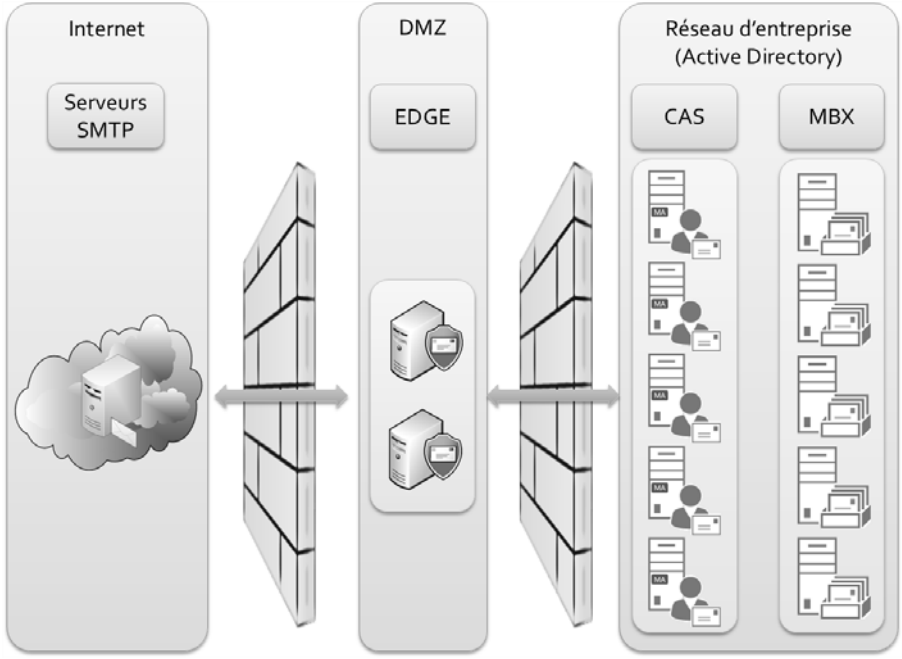
Après analyse du message, lorsque les serveurs de boîtes aux lettres devant s'échanger le message se trouvent dans des groupes de remise différents, le message est de nouveau acheminé par un échange entre les services de transport de différents serveurs de boîtes aux lettres.

Un connecteur d'envoi sur le serveur de boîtes aux lettres est configuré pour la remise du courrier à l'extérieur de l'organisation Exchange à travers le serveur hébergeant le rôle d'accès client.

Même s'il n'est pas encore disponible dans sa version 2013, le rôle **Edge** des précédentes versions d'Exchange peut être utilisé pour permettre une analyse du flux de message en **DMZ** (zone démilitarisée).

Remarque

L'implémentation du serveur Edge sera traitée dans le chapitre Implémentation du rôle Transport Edge de ce livre.



La plupart des mécanismes d'échanges au sein de l'infrastructure Exchange s'appuient sur le protocole **SMTP** (*Simple Mail Transfer Protocol*) comme protocole de transport comme lors des communications avec les domaines de messagerie sur Internet.

1.2 Le protocole SMTP (Simple Mail Transfer Protocol)

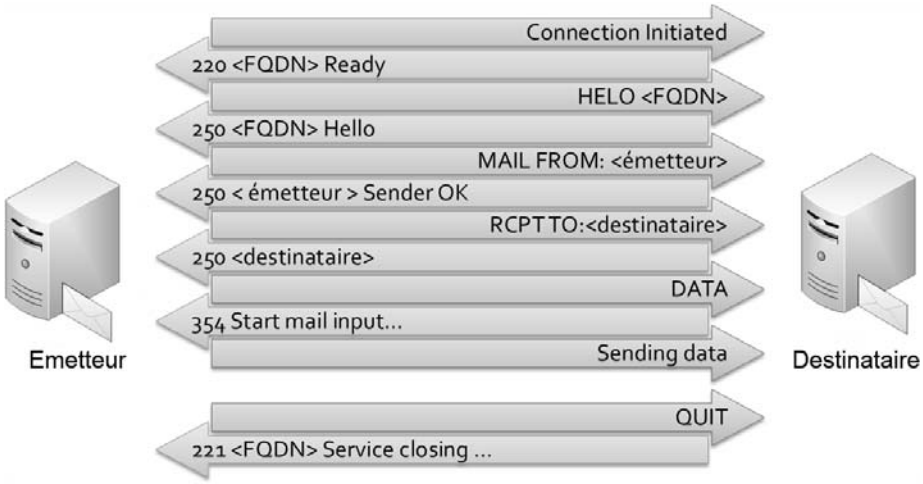
Le protocole **SMTP** assure les fonctions de routage des e-mails, il prend en charge la remise des messages qui lui sont confiés jusqu'à leur destinataire mais peut aussi agir en tant que relais s'il est correctement configuré.

On associe souvent au protocole SMTP un système de file d'attente. En effet, l'un des gros avantages du protocole et qu'il est fondamentalement asynchrone. Si j'envoie un e-mail à mon serveur SMTP et que celui-ci ne peut le remettre immédiatement car le serveur SMTP de destination est en maintenance pendant plusieurs heures, le message va être stocké dans une file d'attente et mon serveur tentera de remettre mon message régulièrement.

Le protocole SMTP utilise le port TCP 25 par défaut, il est devenu le protocole standard de transfert des messages électroniques entre les serveurs et avec les clients.

Comme son nom l'indique (*Simple Mail Transfer Protocol*), le protocole est très basique et n'avait pas pour objectif lors de sa conception de devenir la norme de transfert des e-mails au niveau mondial. Aussi, il présente plusieurs problèmes de conception majeurs particulièrement au niveau de la sécurité et de la montée en charge. L'implémentation d'un serveur SMTP demande donc une attention particulière afin d'éviter que votre serveur devienne la passerelle de relais préférée des spammeurs.

Voici un exemple d'échanges classiques entre deux serveurs de messagerie utilisant le protocole SMTP.



Voici une liste des commandes SMTP les plus courantes :

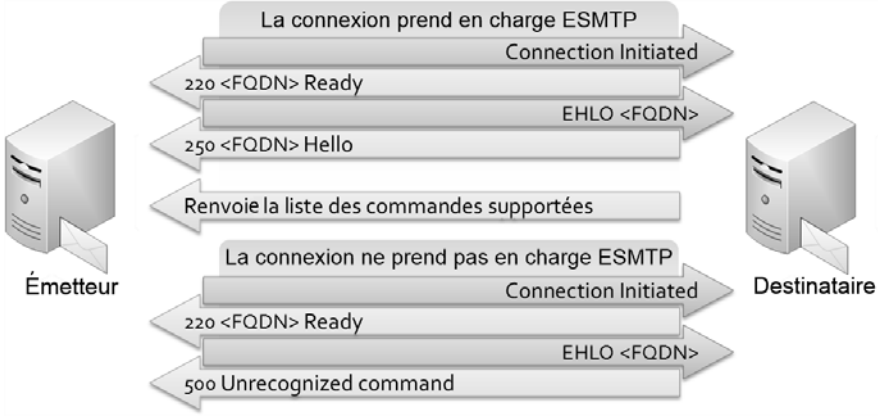
– **HELO <fqdn>** : identifie le serveur émetteur.
– **MAIL FROM:<émetteur>** : identifie l'émetteur du message.
– **RCPT TO:<destinataire>** : identifie le destinataire du message.
– **DATA** : envoie le message au serveur de destination.
– **RSET** : abandonne l'envoi du message en cours.

– **VRFY <chaîne>** : vérifie que le destinataire est valide sur le serveur de destination (cette commande est souvent bloquée pour éviter la constitution d'une liste de spam facilitée).
– **HELP** : affiche la liste des commandes SMTP supportées.
– **QUIT** : déconnecte la session.
– **TURN** : envoie les messages en liste d'attente.

1.3 Le protocole ESMTP (Extended Simple Mail Transfer Protocol)

Afin de combler les manques du SMTP, le protocole **ESMTP** permet d'étendre les commandes SMTP en intégrant notamment l'authentification d'hôtes et le cryptage. La distinction se fait lors de la connexion qui utilise la chaîne de caractères HELO pour le SMTP et EHLO pour le ESMTP.

Le protocole ESMTP permet au serveur de destination de fournir au serveur émetteur la liste des commandes avec lesquels il est compatible. Dans le cas où le serveur de destination n'est pas compatible avec le protocole ESMTP, la connexion est rétablie à l'aide du protocole SMTP.



Voici une liste des commandes ESMTP les plus courantes :

- **EHLO <fqdn>** : identifie l'émetteur et le protocole ESMTP.
- **ATRN** : exécutée si la session est authentifiée.
- **ETRN** : identique à TURN mais spécifie l'hôte distant auquel sera remis le message.
- **PIPELINING** : envoie par lot des commandes SMTP sans en attendre la réponse du destinataire.
- **CHUNKING** : envoie des messages MIME de grandes tailles.
- **STARTTLS** : établit une connexion SSL entre le client et le serveur.
- **AUTH** : fournit une forme d'authentification SASL pour s'authentifier à l'aide de Kerberos et de NTLM.

1.4 Mécanisme d'envoi d'un e-mail

Afin d'envoyer un e-mail, il est nécessaire au serveur de messagerie de connaître l'adresse IP du serveur SMTP de destination. Pour cela il peut choisir entre déléguer la remise à un smart-host ou remettre le message lui-même.

Dans le cas de la délégation de remise, l'ensemble des e-mails devant être envoyés vont être transférés à un autre serveur SMTP qui sera en charge de la remise finale au serveur de destination. Ce rôle peut être assimilé au rôle Edge dans l'infrastructure Exchange 2013.

Dans le cas de la remise directe, le serveur SMTP va interroger l'espace de nom DNS du domaine de destination. Si j'envoie un e-mail à lthobois@editions-eni.fr, le serveur va interroger l'espace de nom editions-eni.fr. Dans l'espace de noms DNS, le serveur SMTP émetteur va rechercher une entrée de type MX qui représente l'un des serveurs de messagerie du domaine distant. Le serveur DNS va alors renvoyer l'adresse IP du serveur de messagerie de destination et lui envoyer l'e-mail.

Une fois l'e-mail envoyé se pose la problématique de la confiance accordée par le serveur de destination à notre e-mail. Cette confiance dépend en partie du contenu de l'e-mail mais aussi de la confiance accordée au serveur émetteur. Si cette confiance n'est pas assez élevée, le message risque d'être catalogué comme spam.