h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

MICROSOFT EXCHANGE

Thèse présentée par

Jardon-El Hiny Noureddine

pour l'obtention du titre de

Bachelor of Science HES-SO en

INGÉNIERIE DES TECHNOLOGIES DE L'INFORMATION AVEC ORIENTATION EN COMMUNICATIONS, MULTIMÉDIA ET RÉSEAUX

PRINTEMPS 2014

Professeur HES Responsable TB
Litzistorf Gérald

h e p i a

Haute école du paysage, d'ingénierie
et d'architecture de Genève

Printemps 2014
Session de bachelor

INGÉNIERIE DES TECHNOLOGIES DE L'INFORMATION

ORIENTATION - COMMUNICATIONS, MULTIMEDIA ET RESEAUX

MICROSOFT EXCHANGE

Descriptif :

Le produit Microsoft Exchange Server est fréquemment utilisé comme serveur de messagerie avec des clients légers (navigateur Internet), lourds (Microsoft Outlook) et terminaux divers (ActiveSync).
La **première partie** du travail (proposée par SIACG) concerne la mise en œuvre d'une messagerie sécurisée et l'échange de messages signés numériquement avec les recommandations sécuritaires de l'éditeur et bonnes pratiques :
- Avantage et inconvénient de la mise en œuvre d'une infrastructure PKI interne à l'entreprise.
- Pourquoi choisir plutôt l'une ou l'autre des deux variantes (S/MIME et PGP) ?

Dans la **seconde partie** (proposée par SmartBee), l'étude portera sur La haute disponibilité des services de messagerie des différents rôles des serveurs Exchange :
- Quel mécanisme utiliser pour les rôles du serveur Exchange (CAS, MB) ?
- Quelle architecture devrait être mise en œuvre dans une configuration minimum (2 serveurs) ?
- Valider la haute disponibilité des services pour le trafic SMTP, l'accès web (OWA), les clients Outlook, les clients ActiveSync
- Quel impact sur la gestion des certificats SSL ?

Travail demandé :

Cette étude comprend les étapes suivantes :

1. Etude théorique **partie 1** à partir des documents officiels et d'articles de qualité
2. Définition du lab de test avec PKI Windows privée composée d'un serveur d'autorité et un serveur subordonné. Deux serveurs Exchange pour dissocier les rôles principaux « Mailbox » et « Client Access ». Deux utilisateurs - boîtes aux lettres.
3. Variante 1 = Messagerie signée puis signée et chiffrée (S/MIME)
   Configuration complète avec serveur Exchange et Outlook + tests unitaires
   Interaction avec Mobile (Android et/ou Iphone)
4. Variante 2 / Messagerie signée puis signée et chiffrée (PGP)
   Config + tests unitaires
5. Etude théorique **partie 2** à partir des documents officiels et d'articles de qualité
6. Définition du lab de test avec maximum 2 serveurs Exchange 2013 pour assurer la redondance
7. Mise en œuvre et tests
8. Bonnes pratiques

Sous réserve de modification en cours du travail de Bachelor

Candidat :
M. Jardon-El-Hiny Nourredine
Filière d'études : ITI

Professeur(s) responsable(s) :
Litzistorf Gérald

En collaboration avec : SIACG & SmartBee
Travail de bachelor soumis à une convention de stage en entreprise : non
Travail de bachelor soumis à un contrat de confidentialité : non

Timbre de la direction

Résumé : Microsoft Exchange

Microsoft Exchange est un logiciel de messagerie propriétaire de Microsoft, fréquemment utilisé par de grandes sociétés ainsi que dans le Cloud. Ce logiciel a été conçu pour l'échange du courrier, la gestion des calendriers et des contacts. Toutes les informations sont stockées dans une base de données sur le serveur et sont accessibles à partir d'un grand nombre de systèmes clients : appareils mobiles, clients lourds Outlook, interface web, etc…

Le but de ce travail a été, dans un premier temps, d'étudier théoriquement le fonctionnement de la version Exchange 2013 SP1 sur un Windows Server 2012 Standard R2 (cette version étant bien différente dans sa conception et son fonctionnement des versions précédentes, notamment de celles de 2007 et 2010) puis, dans un second temps, de la mettre en œuvre suivant plusieurs scénarios.

Le projet s'est déroulé sur 10 semaines, en plusieurs étapes :

1. Lecture de documents officiels Microsoft sur Exchange 2013
2. Etude des flux des protocoles HTTPS et SMTP
3. Etude des différents rôles d'Exchange 2013
4. Installation et configuration des serveurs Windows et Exchange
5. Installation et configuration de différents services, notamment de l'AD, du DNS, de la PKI, des GPOs, pfSense et du cluster Windows
6. Définition de scénarios de tests pour vérifier le bon fonctionnement de l'architecture.

Trois scénarios on été retenus, à savoir :

1. Scénario 1: **Intranet** – Installation d'une infrastructure de messagerie interne sécurisée par le biais de certificats délivrés par une autorité de certification privée. Cette partie comporte:
    a. Une chaîne de certification et les rôles des certificats
    b. Les étapes d'installation et de configuration des différents systèmes et services
    c. Des scénarios de tests des procédures de déploiement des certificats, de signature et de chiffrement

2. Scénario 2 : **Internet** - Transmission de messages sécurisés sur Internet par le biais de certificats. En plus du scénario 1, cette partie comporte des notions :
    a. De pare-feu
    b. De connecteurs Exchange
    c. De flux DNS, HTTPS et SMTP
    d. De gestion des certificats, de tests de signature et de chiffrement sur Internet

3. Scénario 3 : **Haute disponibilité** - Mise en œuvre d'un système de haute disponibilité pour la messagerie. En plus des scénarios 1 et 2, cette partie comporte des notions :
    a. De failover pour le rôle CAS pour les connexions des clients
    b. De mise en cluster pour le rôle MBX pour les bases de données
    c. Des scénarios de tests de différentes pannes
    d. Une configuration supplémentaire sans failover pour le CAS, mais avec du RR
    e. Une configuration supplémentaire avec un MX secondaire

Diplômant :
JARDON-EL HINY NOUREDDINE

Filière d'études : Télécommunications
Ingénierie des Technologies de l'Information

Timbre de la direction

Remerciements

Je tiens à exprimer ma reconnaissance à la Haute école du paysage, d'ingénierie et d'architecture de Genève où j'ai passé trois années de formation qui ont confirmé mon vif intérêt pour les technologies de l'information, en particulier pour les problèmes de sécurité.

Je remercie en particulier M. Litzistorf tout d'abord d'avoir accepté ma suggestion de faire le travail de bachelor sur un sujet qui m'a paru particulièrement intéressant du fait qu'il porte sur une technologie ayant actuellement de multiples applications potentielles et de m'avoir proposé un programme de travail correspondant. Je le remercie aussi pour les pistes de réflexion qu'il m'a suggérées et les nombreux conseils qu'il m'a donnés tout au long de l'exécution de ce projet et de la rédaction du présent rapport.

Je remercie de même MM. Liaudat et Good qui m'ont fait part des besoins auxquels il fallait que mon travail réponde pour être utile en exploitation et qui, par leurs conseils, ont contribué à la réussite de ce travail.

Je remercie également ma famille qui n'a cessé de m'encourager tout au long de mes études et qui m'a supporté avec patience durant l'élaboration de ce rapport.

Je remercie enfin mes amis et mes camarades d'étude de l'amitié qu'ils m'ont accordée ainsi que des encouragements et du soutien dont ils ont fait preuve tout au long de ces années.

Table des Matières

Scénario 1 : Intranet

Scénario 2 : Internet

Scénario 3 : Haute Disponibilité

Scénario 1

Intranet

Emails signés & chiffrés

I/ Introduction

1.1) Contexte

Ce projet a pour but de mettre en œuvre une infrastructure de messagerie basée sur les produits Microsoft Windows Server 2012 & Exchange 2013. Ce travail se fera dans la salle de laboratoire de l'HEPIA afin de pouvoir effectuer les différentes installations de logiciels et de systèmes d'exploitation, les configurations et les tests avant une éventuelle mise en production. Une PKI sera installée afin de bénéficier des possibilités de non-répudiation, de contrôle d'intégrité (Scénario 1.a) et de chiffrement (Scénario 1.b) et de la combinaison des deux (Scénario 1.c) des mails grâce à l'utilisation de certificats. La problématique de la sécurité (firewall, antivirus, anti-spam, sauvegarde, tolérance de pannes) ne sera pas traitée à ce stade.

1.2) Schéma

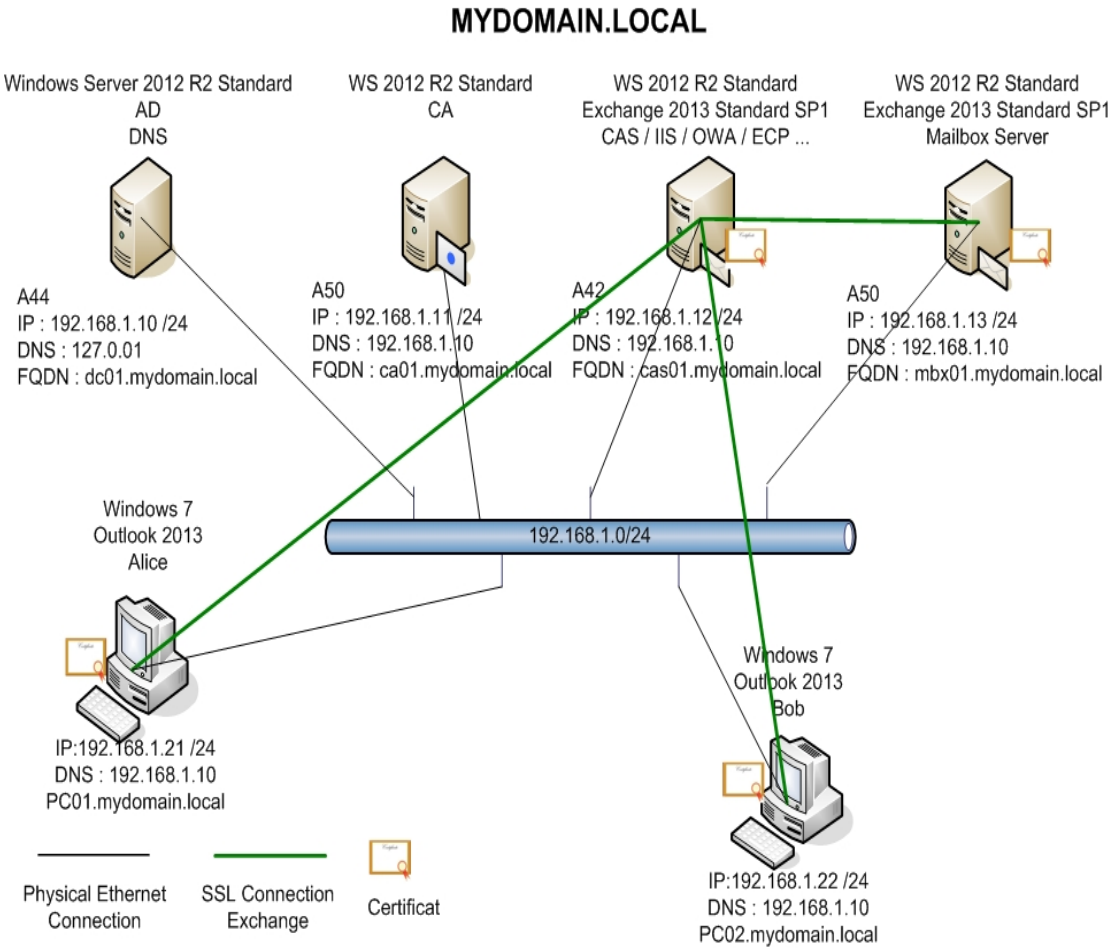


Figure 1 : Schéma de l'installation

1.3) Analyse

Dans ce Scénario 1, il est important de définir le fonctionnement exact de la PKI mise en place. Pour cela, il faut se poser les questions suivantes:

- Quel est le rôle des certificats ?
- Combien de certificats par utilisateur/machine ?
- Comment distribuer les certificats aux serveurs Exchange ?
- Comment distribuer les certificats aux utilisateurs ?
- Quelles informations véhiculent ces certificats ?
- Comment les déployer ?
- Comment imposer l'utilisation de ces certificats ?
- Quels problèmes soulève la perte des clefs privées ?

Il est important de définir exactement le rôle de chaque certificat qui doit être précis et non pas général pour éviter toute utilisation sans discernement.

Les serveurs Exchange possèdent à la base des certificats auto-signés qu'il faudrait, en tout cas pour le serveur CAS, remplacer par un certificat machine délivré par l'autorité de certification pour les services offerts par Exchange. En effet, tous les clients se connectent exclusivement sur ce serveur et il faut éviter l'apparition de messages d'erreurs de sécurité.
Les serveurs utilisent ces certificats à des fins d'authentification et de chiffrement des connexions.

Combien de certificats faut-il attribuer aux utilisateurs?
L'utilisation de deux certificats et de deux clefs privées est obligatoire.
Les clients utilisent leurs certificats à des fins de signature (non-répudiation, intégrité des messages) et de chiffrements des mails et des pièces-jointes.
Nous passons par un mécanisme de dual key. En effet, les exigences en matière de sécurité sont très différentes pour le chiffrement et pour la signature.
Les clefs privées pour la signature ne doivent pas être sauvegardées afin d'assurer la non-répudiation
Par contre, les clefs privées pour le chiffrement doivent obligatoirement être archivées pour éviter les pertes de données en cas de perte ou de corruption de la clef. Comment assurer cela ?

Au laboratoire, il y a un petit nombre d'utilisateurs, mais dans une société, la problématique est différente. Comment s'assurer que tous les collaborateurs ont bien leurs certificats ? Il est important de définir un mécanisme de déploiement automatique des certificats aux utilisateurs du domaine. Ceci peut se faire en utilisant des GPOs comme on le verra par la suite.
Il en est de même pour l'utilisation des certificats. Il faut s'assurer que les employés de l'entreprise signent et chiffrent leur courrier en configurant correctement Outlook 2013 par les GPOs.

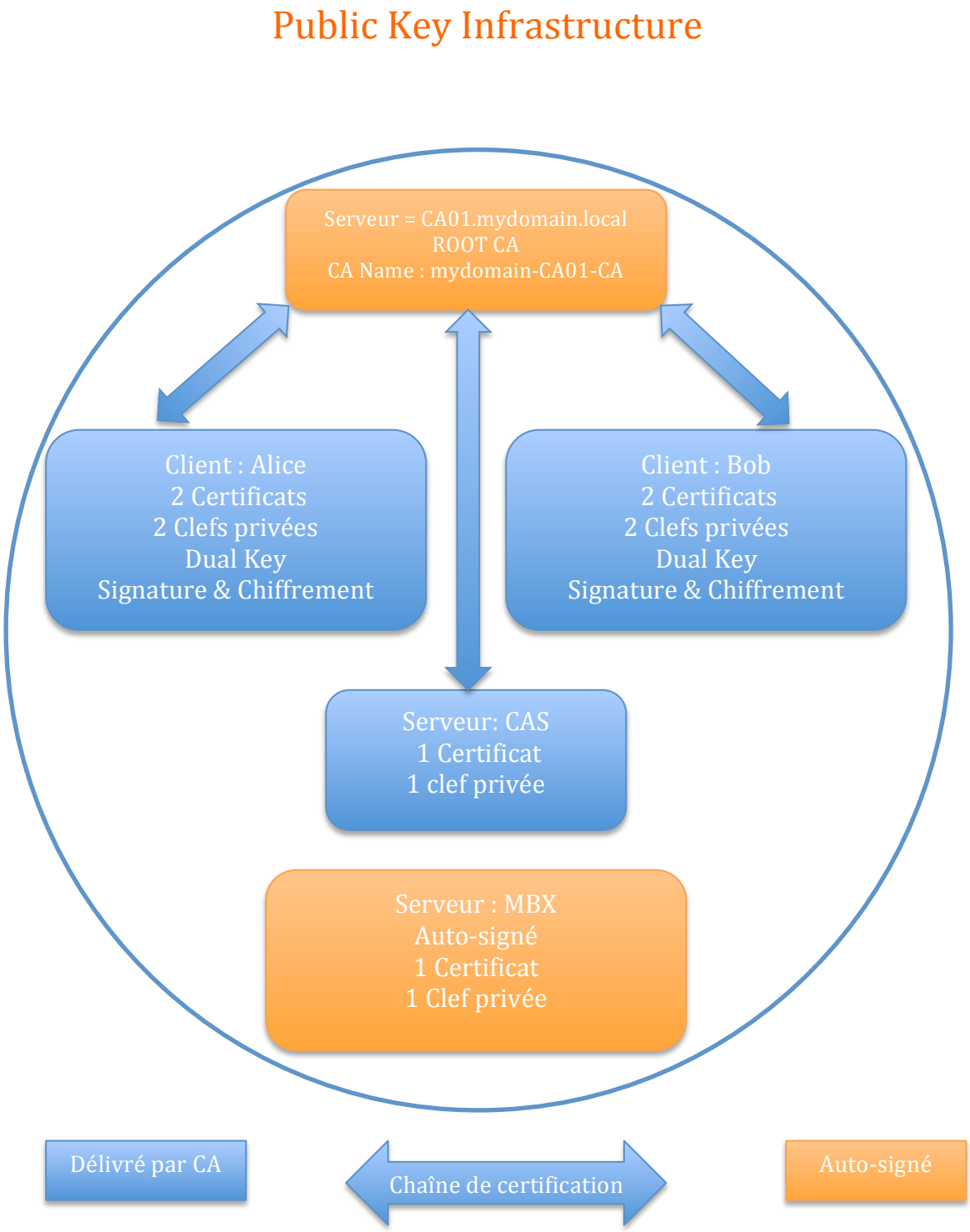
II/ Scénario 1.a (Signature)

2.1) Cahier des charges

Les différents services, logiciels, matériels et autres prérequis pour la mise en œuvre d'une messagerie sont les suivants:

- Un nom de domaine = mydomain.local
  - Nom choisit arbitrairement, mais doit être unique sur le réseau.
- Zone DNS = mydomain.local
  - Lors de l'installation de l'AD, le service DNS et la zone sont installés et créés automatiquement. Mais il est également possible de tout faire manuellement.
- Correspondance obligatoire : nom de domaine Windows et zone DNS (zone DNS de type : AD Integrated)
- Un serveur Active directory (DC01.mydomain)
- Enregistrement des records A des serveurs et postes clients (automatique pour les membres du domaine) et MX (manuel pour le serveur Exchange)
- Un Mailbox Server (Exchange Server 2013 SP1) (MBX01.mydomain
- Un Client Access Server (idem) (CAS01.mydomain)
- Une autorité de certification (CA01.mydomain)
- Windows Server 2012 Standard pour tous les serveurs
- 2 postes clients membres du domaine avec Windows 7 et Outlook 2013
- Déploiement automatique des certificats par GPO
- Délivrance de certificats clients pour la signature des mails
- Nombre de certificats :
  - Postes clients, 2 certificats : 1 personnel pour la signature + celui de la CA à mettre dans le « trusted root certificate store »
  - Serveurs Exchange, 2 certificats : 1 personnel pour les connexions SSL + celui de la CA à mettre dans le « trusted root certificate store »
- Ces certificats permettrons d'assurer:
  - le contrôle d'intégrité des mails échangés
  - la non-répudiation
  - la connexion SSL entre : clients – CAS / CAS - MBX

2.2) Chaîne de certification



2.3) Rôle des certificats

2.4) Etapes d'installation

2.4.0) Obtention des logiciels

M. Bellido a fourni 3 CDs :
- Windows Server 2012 R2 Standard
- Microsoft Exchange 2013 SP1
- Microsoft Outlook 2013

2.4.1) Installation Windows

L'installation de Windows Server 2012 R2 Standard se fait sur :
- PC A44, hébergeant les services et bases de données AD et DNS
- PC A50, hébergeant la CA
- PC A42, hébergeant le rôle CAS d'Exchange
- PC A49, hébergeant le rôle MBX d'Exchange

Pour faciliter les opérations, il est préférable d'installer la version GUI du système et non la core, en ce qui concerne les serveurs hébergeant l'AD et la CA. Il faut savoir que pour les serveurs avec Exchange d'installé, la version de Windows Server 2012 GUI est obligatoire.
Les 4 serveurs seront en GUI pour faciliter les opérations.

Procédure d'installation de Windows :
http://blogs.msdn.com/b/msgulfcommunity/archive/2013/03/06/installing-and-activating-windows-server-2012- step-by-step.aspx
https://www.youtube.com/watch?v=ScSJMfG5R1Y

Adressage IP
Se référer au schéma

Firewall : la problématique du pare-feu n'est pas traitée dans ce scénario. Toutefois, les pare-feu sont activés automatiquement et des règles sont créées par l'OS pour le fonctionnement des différents services.

2.4.2) Installation de l'AD et du DNS

L'installation de l'AD reste triviale dans notre cas et il n'y a rien à rajouter par rapport à la procédure suivante :
http://social.technet.microsoft.com/wiki/contents/articles/12370.step-by-step-guide-for-setting-up-a-windows-server-2012-domain-controller.aspx

En ce qui concerne le DNS, deux cas sont possibles :
- Installation et configuration automatiques
- Installation et configuration manuelles

La procédure d'installation du DNS et de la zone est automatique si, lors de l'installation de l'AD, celui-ci ne trouve pas de zone correspondant au nom de domaine Windows ou s'il n'existe pas de serveur DNS.

Pour procéder à une installation et à une configuration manuelles du DNS, il aurait fallu installer le service DNS en premier, puis l'AD.

La procédure d'installation et de configuration est donc différente,, mais le résultat ne diffère pas (sauf configuration DNS non standard). Afin de réduire au minimum le nombre d'étapes et d'avoir le moindre risque d'erreurs de configuration, il est conseillé de suivre la procédure automatique.

Dans le cas présent où il n'y a aucun serveur DNS, c'est la procédure automatique qui a été choisie pour le service DNS.

Les instructions d'installation pas à pas se trouvent sur le lien ci-dessous. On trouvera juste en dessous les éléments de configuration à remplacer par rapport à la procédure (sections configuration AD et configuration DNS):
http://social.technet.microsoft.com/wiki/contents/articles/12370.step-by-step-guide-for-setting-up-a-windows-server-2012-domain-controller.aspx

2.4.3) Configuration AD

Eléments de configuration AD :

- Création d'une nouvelle forêt
  - Obligation d'avoir une forêt lors de la configuration d'un premier domaine. Un domaine doit appartenir à une forêt
- Root Domain Name : mydomain.local
  - Nom choisi arbitrairement, mais doit être unique sur le réseau
- Forest Fonctional Level : Windows Server 2012 R2
- Domain Fonctional Level : Windows Server 2012 R2
  - Ces deux éléments situés plus haut permettent d'avoir un certain nombre de fonctionnalités AD. Plus de fonctionnalités au niveau 2012 que 2003. Différences expliquées avec ce lien.
  - http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels
- Ajout de ce domaine dans le DNS (Création du DNS automatique)
  - Nous sommes en mode automatique. Pas de DNS existant
- Ce serveur est un GC
  - Obligation d'avoir un Global Catalogue. Il permet de recenser les attributs des objets AD d'autres domaines quand cela s'applique
- Mot de passe DSRM : HEpia10
- NetBIOS name : MYDOMAIN
  - NetBIOS toujours utilisé chez Windows. Ici, il est utilisé afin de vérifier si le nom de domaine est unique sur le réseau.

Voir Annexe : 9.2) Contenu AD

2.4.4) Configuration DNS

Etant donné que nous avons une configuration automatique, avec une zone DNS de type AD Integrated par défaut, les records A des ordinateurs (pour les membres du domaine uniquement) sont dynamiquement insérés dans la base DNS. Annexe 9.3) Contenu DNS
Nous n'avons qu'une entrée à rajouter dans la zone mydomain.local, un record MX pointant sur le CAS :

- MX Record : name : (same as parent folder), type = mx, Data : [10] cas01.mydomain.local

Cette zone est obligatoire, car elle permet aux objets AD de se « trouver ». Localisation du contrôleur de domaine, par exemple.

2.4.5) Installation Windows 7

Procédure d'installation Windows 7
http://www.petri.co.il/ultimate-guide-to-installing-windows-7.htm
NTP : la synchronisation de l'horloge des postes clients (très important) se fait automatiquement avec le contrôleur de domaine.
Vérification de la source de temps (le résultat devrait pointer sur le contrôleur de domaine) : *w32tm /query /source*
Si la source pour le client n'est pas le contrôleur de domaine alors il faut exécuter cette commande : *w32tm /config /syncfromflags:domhier /update*
Vous trouverez le détail ici.

2.4.6) Intégration au domaine

Maintenant que les systèmes d'exploitation clients, les serveurs, ainsi que les différents services sont installés, il faut :

- Tester la connexion ICMP à partir d'un client, par exemple, vers tous les autres systèmes par adresses IP. Si ces tests sont ok, passer à l'étape suivante
- Intégrer les ordinateurs au domaine
- Vérifier l'horloge.. Tous les systèmes doivent avoir la même heure

Procédure :

- Dans la configuration IP des postes clients et serveurs, configurer un serveur DNS statiquement en mettant l'adresse du serveur DNS interne : 192.168.1.10
- Procédure à suivre pour les serveurs :
  - http://mctexpert.blogspot.ch/2012/07/join-windows-server-2012-to-domain-from.html
- Procédure à suivre pour les clients :
  - http://windows.microsoft.com/en-us/windows/connect-computer-domain - 1TC=windows-7
- Eléments de configuration :
  - Machine name (voir schéma)
  - Member of : domain : mydomain.local
  - Username : administrator
  - Password : HEpia10

Une fois l'intégration terminée, faire un test de connectivité ICMP en utilisant les FQDN qu'on peut trouver sur le schéma principal, pour vérifier le bon fonctionnement du DNS.
Il est important également de vérifier la configuration NTP du dc01, pour que tous les systèmes soient synchronisés. Les clients se synchroniseront sur l'heure du dc01 après.[1]

2.4.7) Installation de la CA

Passons à l'installation de la CA. Les instructions d'installation pas à pas se trouvent sur le lien :
Partie 1 : Certificate Authority Server setup
http://4sysops.com/archives/how-to-deploy-certificates-with-group-policy-part-2-configuration/
Voir le paragraphe suivant pour les éléments de configuration à remplacer par rapport à la procédure ci-dessus.

2.4.8) Configuration de la CA

Etant donné que nous sommes dans un Intranet, il faut utiliser une CA privée pour sécuriser l'échange des mails. Grâce à la configuration suivante, la CA pourra générer un certificat root auto-signé qui permettra :

- D'être une autorité de certification root de confiance pour les postes clients
- De signer les certificats que la CA va délivrer aux utilisateurs
- Aux clients de vérifier l'authenticité et l'intégrité des certificats des autres clients (transmis par mail) lors des vérifications de la signature des mails

Pour des raisons de sécurité, il est important d'avoir un algorithme de hachage dont la probabilité de collision est nulle et une clef assez grande pour éviter son craquage..
Ce certificat est généré automatiquement à la fin de la procédure **2.4.7**

Eléments de configuration pour le certificat Root:

- CSP : RSA Microsoft Software Key Storage Provider
  - Choix arbitraire du fournisseur sur la liste recommandée par Microsoft..
- Hash Algorithm : SHA512
  - Spécifie quel algorithme de hachage est utilisé pour signer les certificats que la CA émet
- Key Length : 2048
  - Taille des clefs. Valeur minimale recommandée. Taille plus grande possible, mais peut prendre plus de temps à générer
- CN : mydomain-CA01-CA
  - Common Name permettant d'identifier la CA
- DN : DC=mydomain,DC=local
- Validity Period : 5 years
  - Période de fin de validité du certificat. En général pas trop long pour éviter les problèmes de piratage (clef compromise) et pas trop court pour éviter les renouvellements fréquents.
- Tous ces éléments peuvent être modifiés par l'administrateur lors de la configuration. Ceci est un choix personnel.

[1] http://technet.microsoft.com/en-us/library/cc773263(v=ws.10).aspx

2.4.9) Installation Exchange

Il convient de suivre les instructions d'installation pas à pas. Plusieurs versions sont présentées. Dans notre cas, les étapes d'installation diffèrent en raison de la séparation physique des rôles Exchange puisqu'il y a un rôle CAS sur un serveur, un rôle MBX sur le deuxième alors que, sur ces liens, les deux rôles sont sur le même serveur. NE PAS SUIVRE CELA.

2.4.9.1) Prérequis AD

- *Schema master running Windows Server 2003 with SP2, or a later version of Windows Server*
- *At least one Global catalog server per site that Exchange will be installed in that is running Windows Server 2003 SP2 or later*
- *At least one Domain controller per site that Exchange will be installed in that is running Windows Server 2008 or later*
- *Forest functional mode of Windows Server 2003 or higher*

An account with Schema Admins, Domain Admins, and Enterprise Admins permissions to run Exchange setup[2]

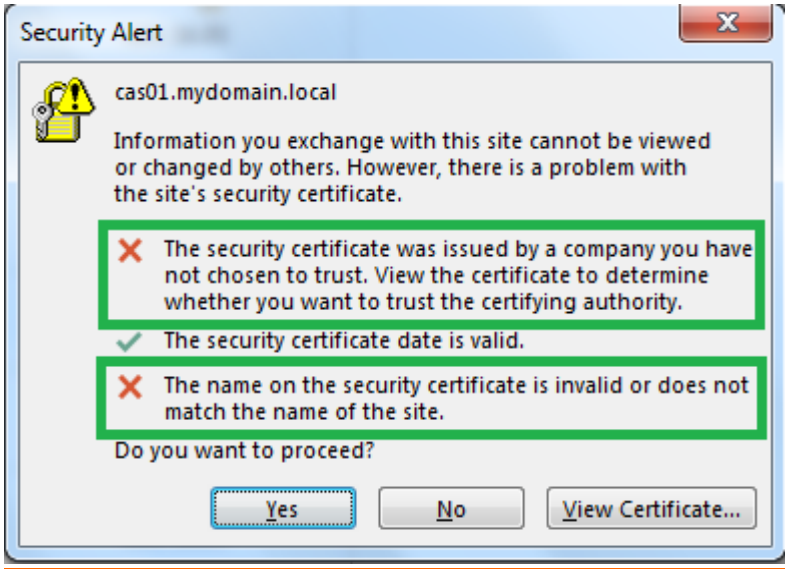
2.4.9.2) Procédure d'Installation Exchange:

Deux procédures d'installation sont possibles, GUI ou CLI. Les procédures sont détaillées dans ces liens. C'est la version GUI qui a été utilisée:

- *http://social.technet.microsoft.com/wiki/contents/articles/14506.how-to-install-exchange-2013-on-windows-server-2012.aspx (GUI)*
- *https://www.youtube.com/watch?v=auircJQPujM (GUI)*
- http://dilshansaminda.wordpress.com/2013/07/17/microsoft-exchange-2013-installation-with-powershell/ (CLI)

[2] *http://exchangeserverpro.com/how-to-install-exchange-server-2013/*

2.4.10) Certificat Serveur CAS



sFigure 2 : Message d'erreur de certificat

Afin d'éviter les messages d'erreur de ce type chez les clients dus à l'utilisation du certificat auto-signé par le CAS, et pour être en mesure d'assurer une meilleure sécurité (révocation, intégrité du certificat CAS et vérification de son authenticité par les clients), il faut délivrer un certificat au CAS. Pour cela, il faut effectuer une requête de certificat à partir de la console d'administration d'Exchange et la soumettre à la CA.

Marche à suivre :
http://exchangeserverpro.com/create-ssl-certificate-request-exchange-2013/
http://technet.microsoft.com/en-us/library/bb125165(v=exchg.150).aspx

Eléments de configuration à remplacer:

- Friendly name : cas01
  - On donne un nom au certificat
- Domains included (définit les différents services Exchange pour lesquels le certificat sera utilisé):
  - OWA (Accès au web mail)
  - OAB (Offline address book)
  - Exchange Web Services
  - Exchange Active Sync (Service pour mobiles)
  - AutoDiscover
  - Outlook Anywhere (RPC over HTTPS)
- Domains (définit les différents FQDN pour lesquels le certificat sera valide):
  - cas01.mydomain.local
  - AutoDiscover.mydomain.local
  - Mydomain.local

Tous ces éléments de configuration définissent tous les services et FQDN d'Exchange qui utiliseront ce certificat.

Une fois la requête sauvegardée, il faut la transmettre à la CA (par clef USB, SMB, etc), puis ouvrir une requête de commande chez la CA, dans laquelle il faut taper la commande suivante afin de générer le certificat :
certreq -submit -attrib "CertificateTemplate:WebServer" <Cert Request.req>
<Cert Request.req> étant le chemin du fichier contenant la requête.
Une fois le certificat délivré après l'exécution de cette commande, il faut le transmettre au CAS (clef USB, SMB, etc) et le mettre dans le container personnel des certificats de la machine. L'importation du certificat dans le store permet de terminer la requête de certificat par Exchange et termine la procédure automatiquement. Le certificat sera tout de suite reconnu par Exchange comme étant valide.
Pour terminer, il faut aller dans la console d'administration d'Exchange et spécifier que le certificat sera utilisé pour les communications SMTP (si l'option TLS est utilisée) et HTTPS.
Annexe 9.8) Certificat Exchange

2.4.11) Certificat Serveur MBX

Cette étape n'est pas obligatoire pour ce serveur qui possède déjà un certificat auto-signé. Pour plus de sécurité, le CA peut lui délivrer un certificat, mais pour le client, cela ne change rien, car il n'y a aucune connexion client-MBX.
Pour obtenir un certificat, il convient de suivre la procédure précédente **(2.4.10).**

2.4.12) Certificats clients

Les clients doivent tenir compte de deux éléments importants, à savoir qu'ils doivent tout d'abord posséder le certificat (clef publique) de la CA, ainsi que leur propre certificat pour leur permettre de signer leurs mails.
Pour cela, il faut créer une OU nommée : Clients où se retrouvent les comptes utilisateurs et les comptes machines. Cette GPO (du nom de certificat) sera liée à cette OU et appliquée à ces comptes dans les 2 étapes suivantes.
Annexe 9.4) Contenu de la GPO

2.4.12.1) Installation du certificat de la CA

Il faut :
- Exporter le certificat root de la CA
- L'importer dans le « Trusted Root Certificates» sur le compte machine des clients en passant par la GPO de l'AD

Marche à suivre :
http://technet.microsoft.com/en-us/library/cc738131(v=ws.10).aspx

2.4.12.2) Certificats clients (signature)

Il faut créer un *«certificate template »*, basé sur un modèle existant : le *« user certificate template »*. Nous l'appellerons le *« mail signing »*.

Marche à suivre (Creating the Certificates) :
http://4sysops.com/archives/how-to-deploy-certificates-with-group-policy-part-2-configuration/
Eléments de configuration :

- Validity period : 1 year
- Publish certificate in Active Directory
- Compatibility
    - CA : Windows server 2012 R2
    - CR : Winsows 7 / Server 2008 R2
        - Ces deux éléments, en fonction des versions des OS des serveurs et clients, permettent d'ajouter de nouvelles fonctionnalités. Un CR de Windows 7 / Windows Server 2008 R2, rajoute des fonctionnalités dans le modèle de certificat qui peuvent ne pas être compatibles avec un client XP, par exemple.
- Purpose : signature
- Enroll subject without requiring any user input
- Security :
    - Enroll & Autoenroll & Read permissions : allowed for Domain Users
- Extensions :
    - Application policies : secure email
- Key Usage :
    - Digital Signature
        - Permet le contrôle d'intégrité du mail
    - Signature is proof of origin
        - Permet la non-répudiation

Une fois le modèle créé, il sera à la disposition des clients dont l'enrôlement sera automatique par le biais de la GPO pour le certificat « mail signing » à l'ouverture de session. Tout cela est bien sûr transparent pour l'utilisateur.
Annexe 9.5.1) Modèle de la signature

2.4.13) Forcer l'utilisation des certificats (GPO)

Il faut maintenant s'assurer que les clients utiliseront leur certificat pour signer les mails ce qui se fait également par le biais des GPO. Par défaut, les GPO ne peuvent pas interférer avec les produits Office. En effet, il n'existe aucun onglet ou menu permettant de gérer Office. Nous devons installer un addon spécifique (les Office Policy Administrative Templates). Cette GPO a été nommée : Certificat.

Marche à suivre :
http://www.howto-outlook.com/howto/policies.htm

Un nouveau menu déroulant dans les GPOs permet de configurer Outlook 2013 pour obliger les clients à utiliser leur certificat pour signer les mails. Aucune action de leur part n'est nécessaire.

Eléments de configuration de la GPO :

- Sign all messages : enabled
- Do not check e-mail address against address of certificates being used : disabled
    - Vérification si l'email de l'émetteur = email dans le certificat
- Signature Warning : enabled : Always warn about invalid signatures
- Request S/MIME receipt for all S/MIME signed messages
    - Oblige le destinataire à envoyer un message pour confirmer que le message :
        - N'a pas été altéré
        - Que la signature a été validée
        - Et indiquer par qui et quand ce mail a été ouvert

Lorsqu'un mail est envoyé, le certificat contenant la clef publique de l'émetteur y est annexée. Il n'y a donc aucune action utilisateur ou administrateur à effectuer. Le certificat est également ajouté dans l'objet (utilisateur) dans la base de données AD.

2.4.14) Création des utilisateurs

Nous pouvons créer des utilisateurs de deux manières différentes :

- En passant par l'AD
- En passant par Exchange directement

Les utilisateurs Alice et Bob ont été créés en passant par Exchange et la procédure :
http://www.techieshelp.com/create-a-new-user-in-exchange-2013/

2.4.15) Installation Outlook 2013

Voici la procédure d'installation de Microsoft Office 2013
http://www.techieshelp.com/office-2013-step-by-step-install-guide/

2.4.16) Configuration compte Exchange

Procédures de configuration

- Manuelle :
    - http://www.colorado.edu/oit/tutorial/exchange-configuration-first-time-outlook-2013-use
    - Remplacer « Server » par : cas01.mydomain.local
- Automatique
    - Ouvrir Outlook 2013
    - Do you want to set up Outlook to connect to an email account ? : yes
    - Sélectionner : email account.
    - La configuration sera automatique (détection automatique du serveur Exchange) et les données d'authentification de logon de l'utilisateur seront utilisées.

III/ Tests Scénario 1.a (Signature)

3.1) Test déploiement du certificat de la CA aux clients

Si tout a été bien configuré lors du démarrage de la machine et si le certificat de la CA n'est pas dans le *« trusted root certificate store»,* alors la GPO l'installera automatiquement. Pour vérifier :

- Ouvrir une requête de commande
- Taper *MMC* pour ouvrir la console de management
- *Fichier-ajout composant logiciels enfichables* : ajouter *certificat*
- Vérifier si le certificat est dans *le trusted root certificate store*
- Délivré à = délivré par (certificat auto-signé)

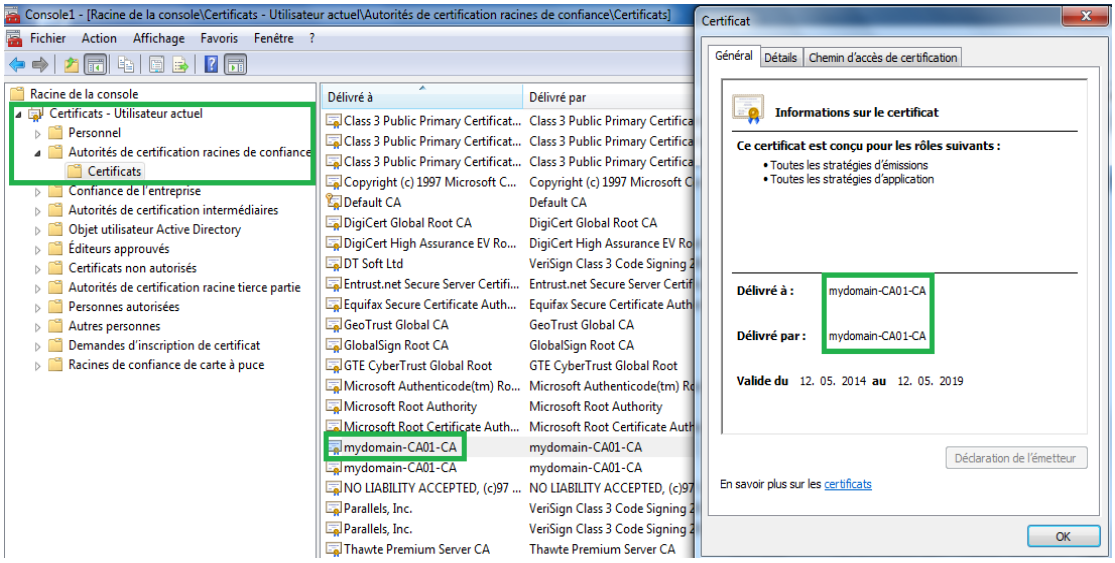


Figure 3 : Vérification présence du certificat de la CA

Nous pouvons observer que tout est bon. Le certificat est bien présent et valide.

3.2) Signature

3.2.1) Test déploiement automatique des certificats clients (Signature)

Si tout a été bien configuré lors du premier logon de l'utilisateur (Bob) et si son certificat personnel n'est pas dans le « personal certificate store», alors la GPO l'installera automatiquement. Pour vérifier :

- Ouvrir une requête de commande
- Taper *MMC* pour ouvrir la console de management
- *Fichier-ajout composant logiciels enfichables* : ajouter *certificat*
- Vérifier si le certificat est dans *le personal certificate store*
- Protège le courrier électronique

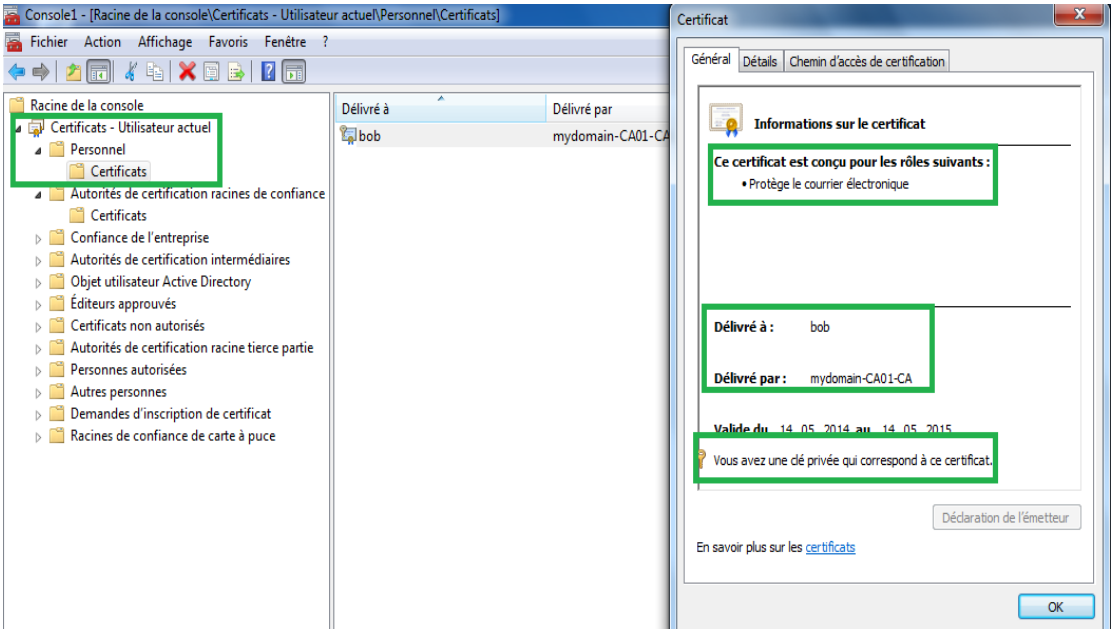


Figure 4 : Vérification délivrance certificat personnel pour signature

Nous pouvons observer que tout est bon. Le certificat est bien présent.

3.2.2) Test obligation d'envoi de mail signé avec accusé de réception

Si tout a été bien configuré au niveau de la GPO, les utilisateurs sont obligés de signer leurs mails. Pour vérifier :

- Ouvrir Outlook 2013
- Fichier-option-trust center-trust center settings
- Les boîtes suivantes seront grisées et cochés :
    - *Add digital signature to outgoing messages*
    - *Request S/MIME receipt for all S/MIME signed messages*
- Nous voyons également que SHA1 est utilisé
- *Send these certificates with signed messages*
    - Permet d'envoyer la clef publique au destinataire afin qu'il puisse vérifier la signature

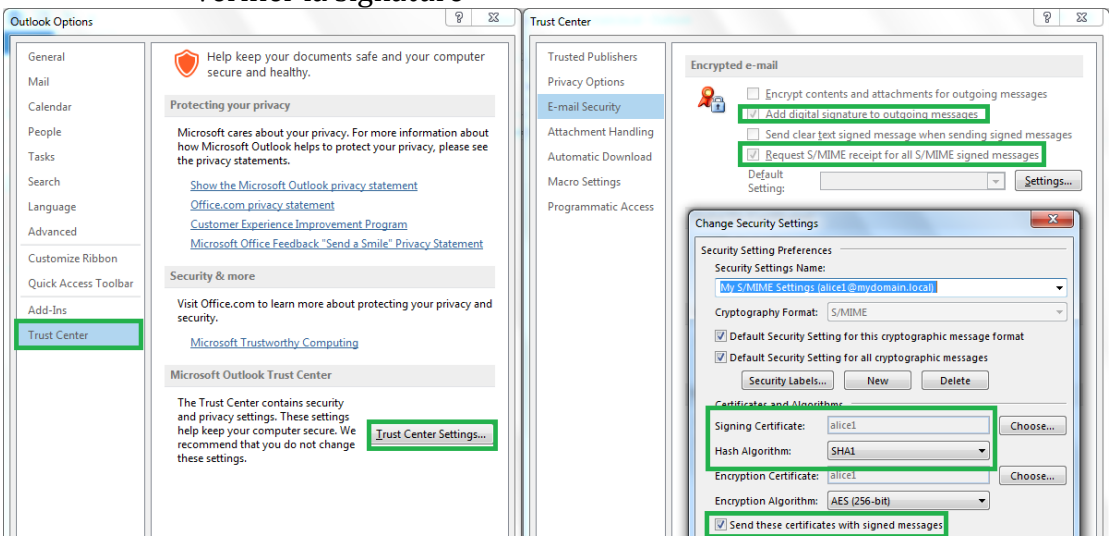


Figure 5 : Vérification paramètres de signature

Nous pouvons observer que tout est bon également

3.2.3) Envoi d'un mail signé et observation du résultat

Bob envoie un mail signé à Alice. Voilà le résultat :

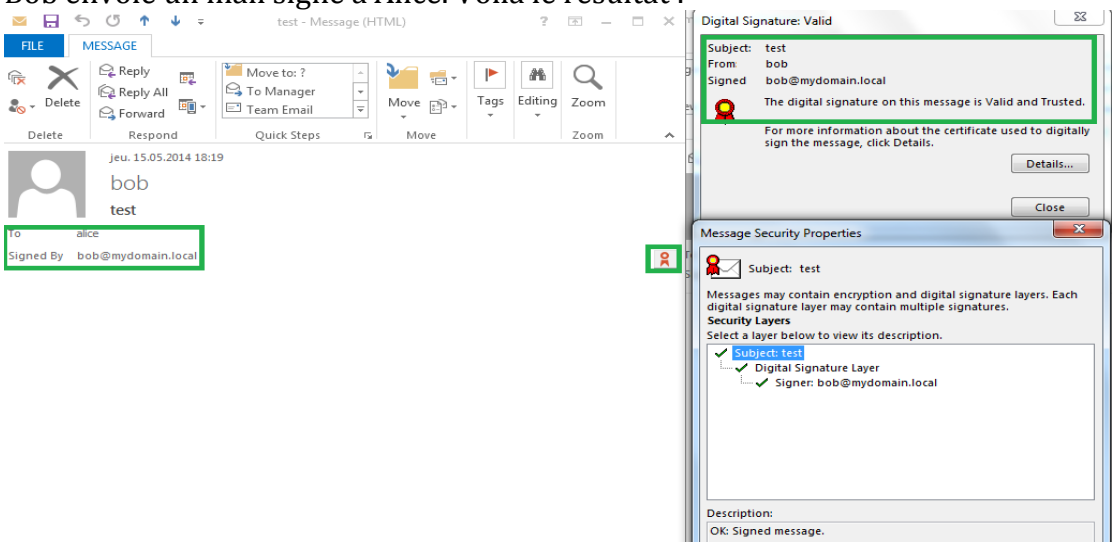


Figure 6 : Vérification signature

Les champs en vert indiquent que le message envoyé par Bob à Alice, est bien signé et que la signature est valide. Il n'y a aucune problème à ce sujet

IV/ Scénario 1.b (Chiffrement)

Ce scénario diffère peu du scénario précédent. Seules les différences sont signalées.

4.1) Cahier des charges

- Pareil que le 2.1
- Suppression du mécanisme de signature
- Ajout d'un mécanisme de chiffrement de mails (contenu et pièces jointes) avec certificat
- Nombre de certificats :
    - Postes clients, 2 certificats : 1 personnel pour le chiffrement + celui de la CA à mettre dans le « trusted root certificate store »
    - Serveurs Exchange, 2 certificats : 1 personnel pour les connexions SSL + celui de la CA à mettre dans le « trusted root certificate store »
- Ces certificats permettent :
    - d'assurer le chiffrement des mails échangés entre les clients
    - d'assurer la connexion SSL clients – CAS / CAS - MBX

4.2) Certificats clients

Veuillez reprendre le point **2.4.12**

4.2.1) Installation du certificat de la CA

Veuillez reprendre le point **2.4.12.1**

4.2.2) Certificats clients (Chiffrement)

Il faut créer un *«certificate template »*, basé sur un modèle existant : le *« mail signing template »*. Nous l'appellerons le *« mail cypher»*.

Marche à suivre (Creating the Certificates) :

http://4sysops.com/archives/how-to-deploy-certificates-with-group-policy-part-2-configuration/

Eléments de configuration :

- Dupliquer le modèle *« mail signing »* et le nommer *« mail cypher »*
- Validity period : 1 year
- Publish certificate in Active Directory
- Compatibility
  - CA : Windows server 2003
  - CR : Winsows XP / Server 2003
- Purpose : encryption
- Enroll subject without requiring any user input
- Security :
  - Enroll & Autoenroll & Read permissions : allowed for Domain Users
- Extensions :
  - Application policies : secure email
- Key Usage :
  - Allow key exchange only with key encryption
    - Permet de générer une clef symétrique, de la chiffrer et de l'envoyer à destination
  - Allow encryption of user data
    - Permet d'utiliser cette clef pour le chiffrement des données

Annexe 9.5.2) Modèle de chiffrement

4.3) Forcer l'utilisation des certificats (GPO)

Veuillez reprendre le point **2.4.13**

Il est possible de forcer les clients à utiliser leur certificat pour chiffrer les mails.

Eléments de configuration de la GPO :

- Encrypt all messages: enabled
- Do not check e-mail address against address of certificates being used : disabled
  - Vérification si l'email de l'émetteur = email dans le certificat
- Request S/MIME receipt for all S/MIME signed messages
  - Oblige le destinataire à envoyer un message indiquant:
    - Que le message n'a pas été altéré
    - Que la signature a été validée
    - Par qui et quand ce mail a été ouvert

Lorsqu'un mail est envoyé, le certificat contenant la clef publique de l'émetteur y est annexé. Aucune action utilisateur ou administrateur n'est donc nécessaire.
Le certificat est également ajouté dans l'objet (utilisateur) dans la base de données AD.

V/ Tests Scénario 1.b (Chiffrement)

5.1) Test déploiement automatique des certificats clients (Chiffrement)

Si tout a été bien configuré lors du premier logon de l'utilisateur et si son certificat personnel n'est pas dans le « personal certificate store», alors la GPO l'installera automatiquement. Pour vérifier :

- Ouvrir une requête de commande
- Taper *MMC* pour ouvrir la console de management
- *Fichier-ajout composant logiciels enfichables* : ajouter *certificat*
- Vérifier si le certificat est dans *le personal certificate store*
- Utilisation de la clef : chiffrement de la clef et des données

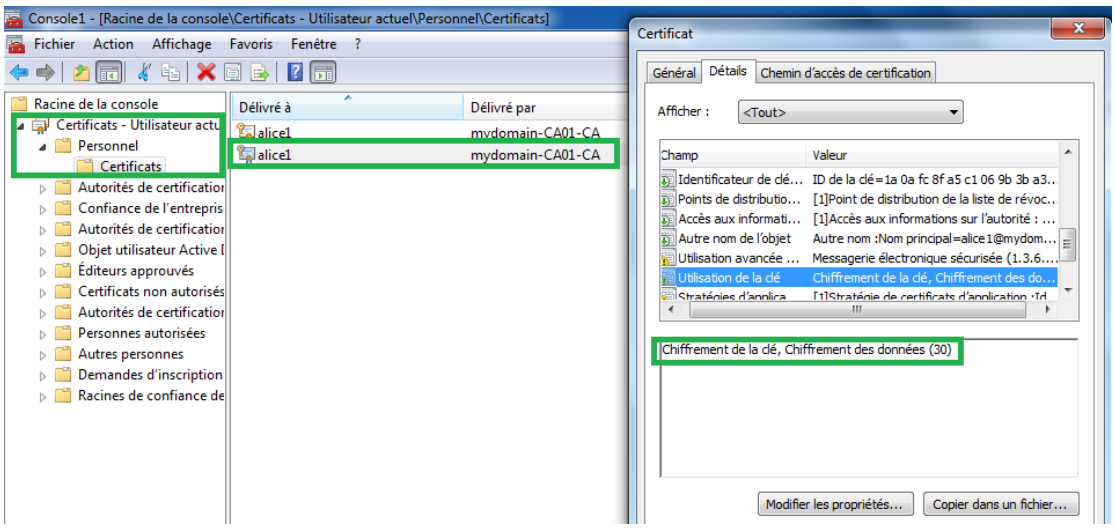


Figure 7 : Vérification délivrance certificat pour chiffrement

Nous voyons que tout est bon. Le certificat est bien présent.

5.2) Test obligation d'envoi de mail chiffré avec accusé de réception

Si tout a été bien configuré en ce qui concerne la GPO, les utilisateurs sont obligés de chiffrer leurs mails. Pour vérifier :

- Ouvrir Outlook 2013
- Fichier-option-trust center-trust center settings
- Les boîtes suivantes seront grisées et cochées :
  - *Encrpyt contents and attachments for outgoing messages*
  - *Request S/MIME receipt for all S/MIME signed messages*
- Nous voyons également que AES-256 est utilisé (pas obligatoire)

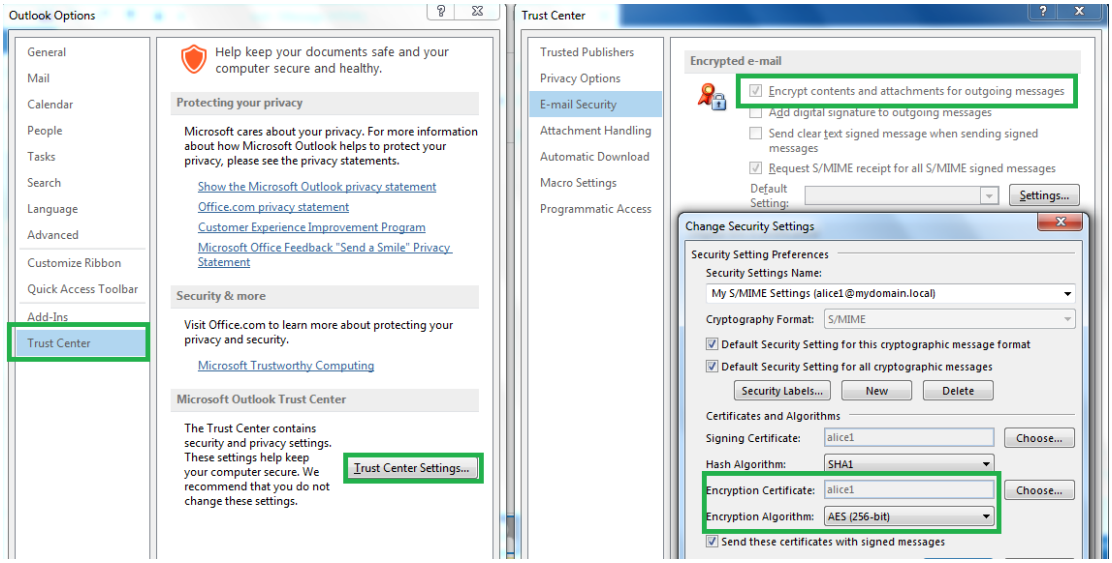


Figure 8 : Vérification paramètres pour chiffrement

5.3) Envoi d'un mail chiffré et observation du résultat

Bob envoie un mail chiffré à Alice. Voilà le résultat :

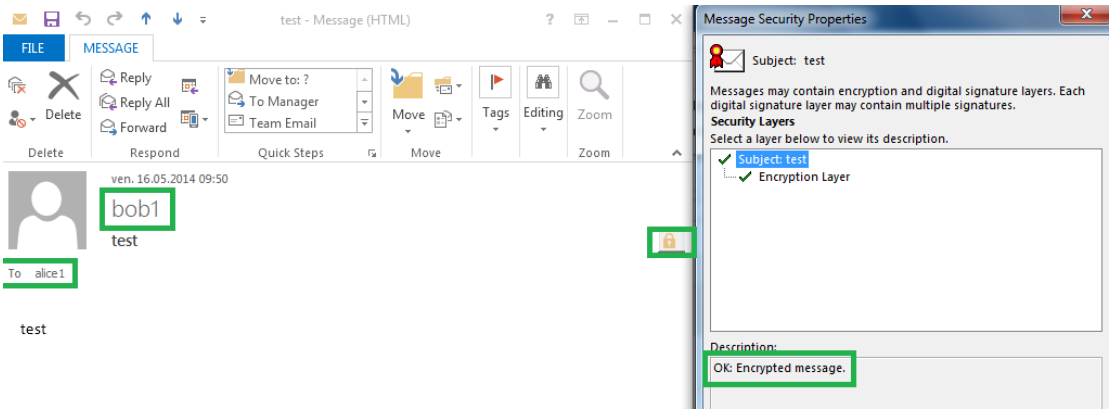


Figure 9 : Vérification chiffrement du mail

Les champs en vert indiquent que le message envoyé par Bob à Alice, est bien chiffré. Il n'y a donc aucun problème. En cliquant sur *« Encryption Layer »*, on peut voir l'algorithme de chiffrement (3DES).

VI/ Scénario 1.c (Signature et chiffrement)

6.1) Cahier des charges

- Pareil que le 2.1 et 4.1
- Garde mécanisme de signature avec certificat
- Garde mécanisme de chiffrement (contenu et pièces jointes) avec certificat
- Nombre de certificats :
    - Postes clients, 3 certificats : 2 personnels (Dual Key) pour la signature et le chiffrement + celui de la CA à mettre dans le « trusted root certificate store »
    - Serveurs Exchange, 2 certificats : 1 personnel pour les connexions SSL + celui de la CA à mettre dans le « trusted root certificate store »
- Ces certificats assurent:
    - le contrôle d'intégrité des mails échangés
    - la non-répudiation
    - le chiffrement des mails échangés entre les clients
    - la connexion SSL entre : clients – CAS / CAS - MBX

6.2) Certificats clients

Reprendre 2.4.12 et 4.2

6.3) Forcer l'utilisation des certificats (GPO)

Reprendre le point **2.4.13**
On pourra forcer les clients à utiliser leur certificat pour signer et chiffrer les mails.

Eléments de configuration de la GPO :

- Sign all messages : enabled
- Encrypt all messages : enabled
- Do not check e-mail address against address of certificates being used : disabled
    - Vérification si l'email de l'émetteur = email dans le certificat
- Signature Warning : enabled : Always warn about invalid signatures
- Request S/MIME receipt for all S/MIME signed messages
    - Oblige le destinataire à envoyer un message indiquant :
        - Que le message n'a pas été altéré
        - Que la signature a été validée
        - Par qui et quand ce mail a été ouvert

Lorsqu'un mail est envoyé, le certificat contenant la clef publique de l'émetteur y est annexé. Aucune action utilisateur ou administrateur n'est donc nécessaire
Le certificat est également annexé à l'objet (utilisateur) dans la base de données AD.

VII/ Tests Scénario 1.c (Signature & Chiffrement)

7.1) Test obligation d'envoi de mail signé et chiffré avec accusé de réception

Si tout a été bien configuré concernant la GPO, les utilisateurs sont obligés de signer et de chiffrer leurs mails. Pour vérifier :

- Ouvrir Outlook 2013
- Fichier-option-trust center-trust center settings
- Les boîtes suivantes seront grisées et cochées :
    - *Encrpyt contents and attachments for outgoing messages*
    - *Add digital signature to outgoing messages*
    - *Request S/MIME receipt for all S/MIME signed messages*
- Nous voyons également que SHA-512 et AES-256 peuvent être utilisés
- *Send these certificates with signed messages*
    - Permet d'envoyer la clef publique au destinataire pour vérification de la signature

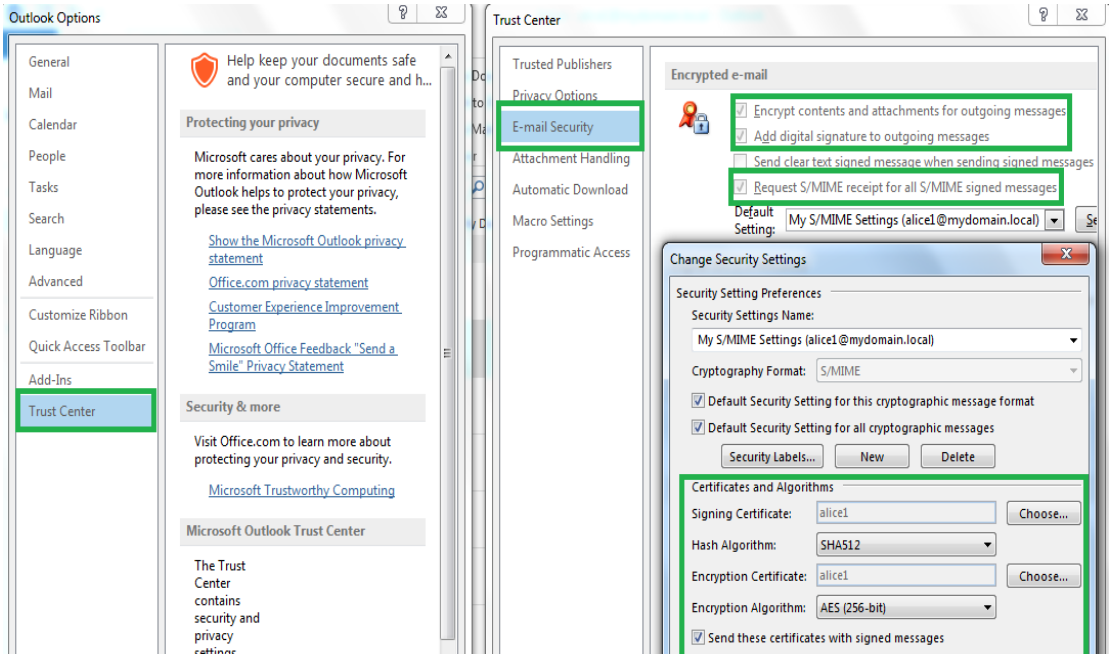


Figure 10 : Vérification paramètres signature et chiffrement

On voit que les parties signature et chiffrement sont grisées et cochées et que les certificats ont été sélectionnés automatiquement pour la signature et le chiffrement.

7.2) Envoi d'un mail signé et chiffré et observation du résultat

Bob envoie un mail signé et chiffré à Alice. Voilà le résultat :

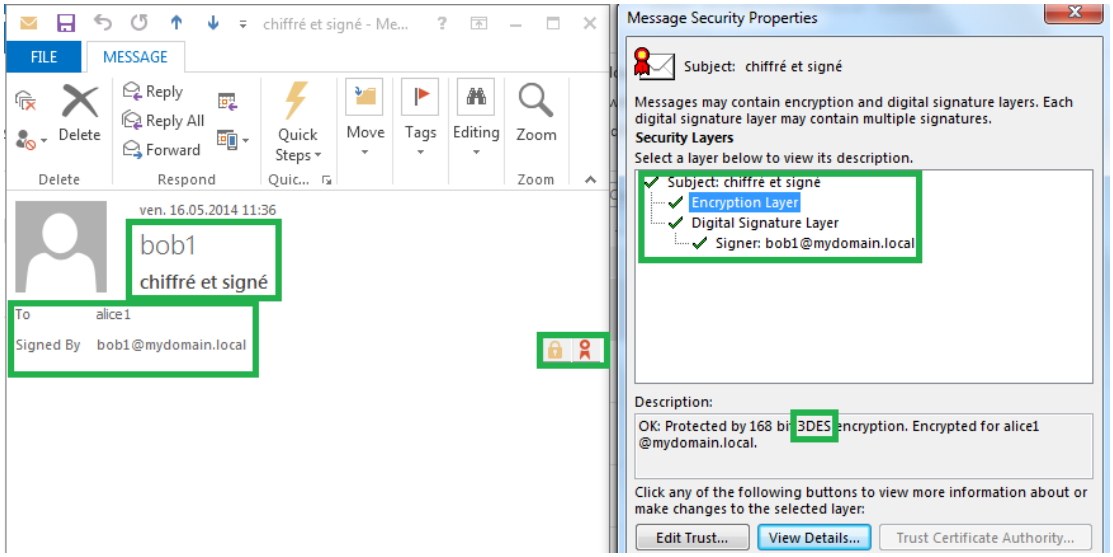


Figure 11 : Vérification si mail signé et chiffré

On voit que le message et son contenu ont été chiffrés avec 3DES

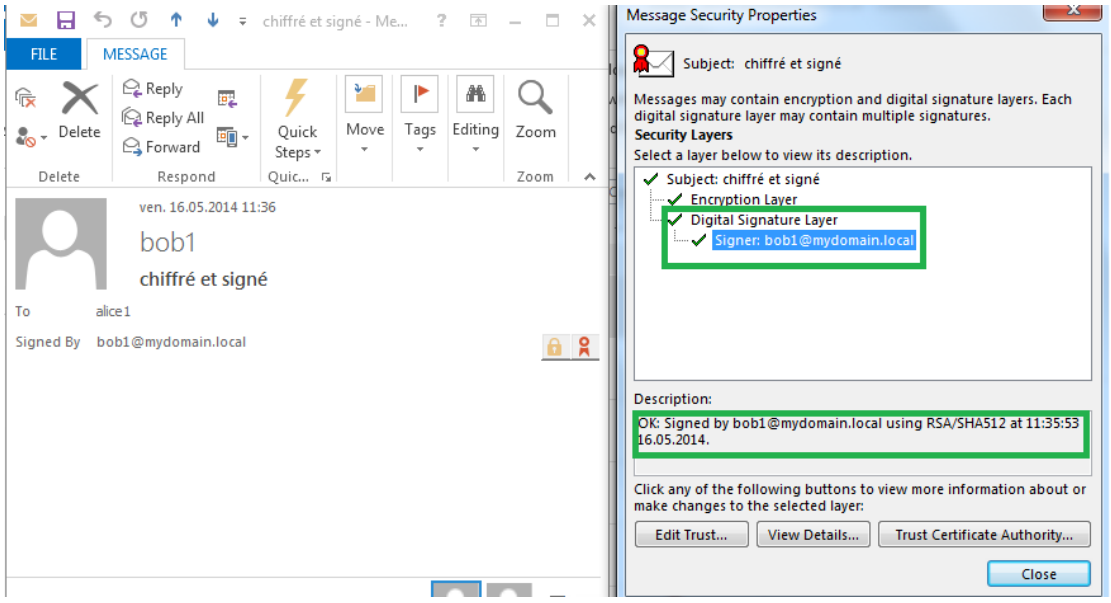


Figure 12 : Vérification si mail signé et chiffré

On voit que le message a été signé avec RSA/SHA-512

VIII/ Conclusion

Cette partie du projet est très intéressante en ce qui concerne les trois scénarios en interne qui ont été proposés (signature, chiffrement, puis signature avec chiffrement) car elle fait appel à beaucoup de notions étudiées en cours, notamment au sujet d'une CA et des certificats. Les connaissances acquises sur ce sujet grâce aux documents techniques Microsoft et aux tests permettent de mieux comprendre la complexité et les fonctionnalités qui se cachent derrière une autorité de certification dans le monde Microsoft dont on découvre la puissance sur ce point et certains éléments complexes à mettre en œuvre.

Cela m'a permis de cerner les processus précis:

- de configuration d'une CA
- de délivrance automatique de certificats (enrôlement automatique)
- des GPO pour les déploiements des certificats et la configuration d'Outlook
- de transmission des clefs publiques grâce à l'infrastructure AD permettant de vérifier les signatures et de chiffrer sans avoir besoin de déployer manuellement les certificats
- de gestion et de modification des modèles de certificats et des différentes options Microsoft
- de mise en place des certificats pour Exchange

A ce stade, le projet m'a beaucoup appris sur le fonctionnement (flux de messagerie, rôle, SSL) d'un produit complexe grâce aux documents Microsoft officiels sur Exchange 2013. Pour le peu qui m'ait été donné de voir jusqu'à présent, j'ai pu observer sans configurer, une partie de la complexité et des fonctionnalités d'un tel logiciel de messagerie.

Dans le cadre d'une configuration interne, l'installation d'Exchange ainsi que la configuration restent assez simples et sont faciles à mettre en place. Le plus important dans cette partie a été de comprendre le fonctionnement d'Exchange avec les différents rôles et de mettre en place le bon certificat pour sécuriser les connections avec les clients avec un certificat délivré par la CA et non le certificat auto-signé de base, afin d'améliorer la sécurité et d'éviter aux utilisateurs les désagréments des messages d'erreur.

Les différents tests finaux concernant la signature, le chiffrement, la mise en place des certificats (en configurant des modèles) et des configurations grâce aux GPOs pour le déploiement automatique des certificats et de la configuration d'Outlook 2013 ont été concluants.

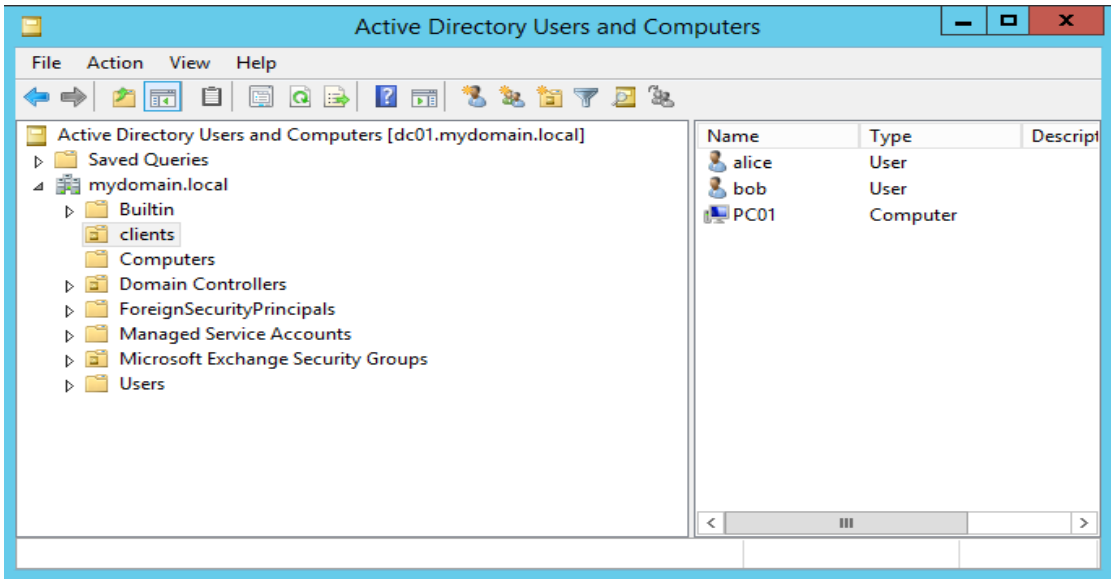
IX/ Annexes

9.1) Choix du système d'exploitation

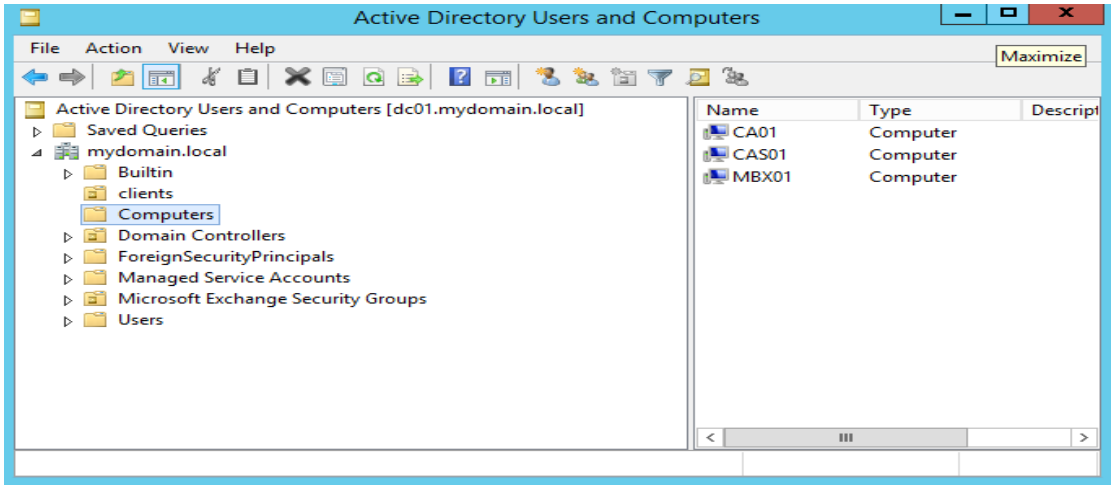
Il a fallu choisir un système d'exploitation serveur extensible en tenant compte d'éléments tels que l'apport de nouvelles fonctionnalités par rapport à d'anciens produits, la durée de vie des produits, les mises à jour, etc… Le système doit être extensible et pouvoir rester fonctionnel le plus longtemps possible sans qu'il soit nécessaire de migrer vers une autre version ou infrastructure à un moment donné en raison d'une mauvaise conception ou d'une mauvaise analyse des besoins (fin de durée de vie, produits incompatibles…).

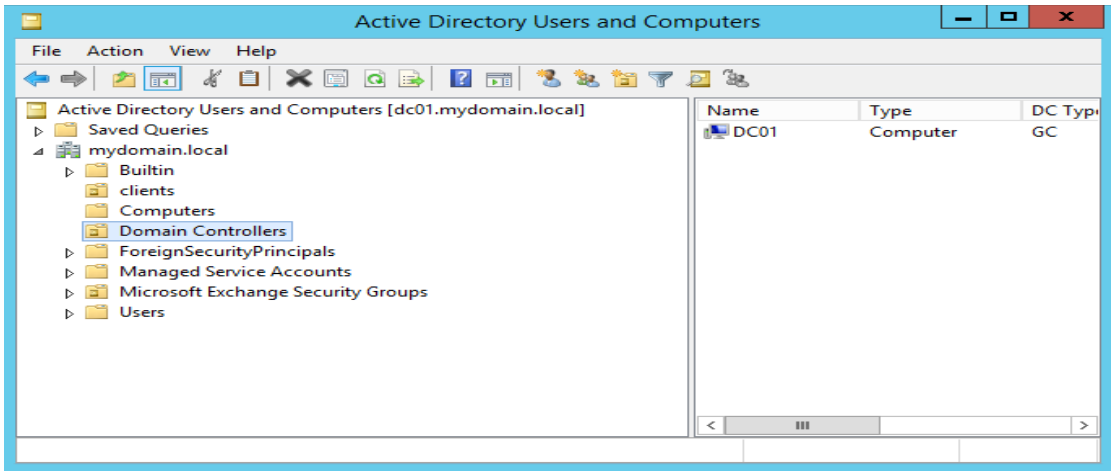
9.2) Contenu AD

Dans les 3 figures suivantes, on retrouve les différentes machines du réseau, membres du domaine.



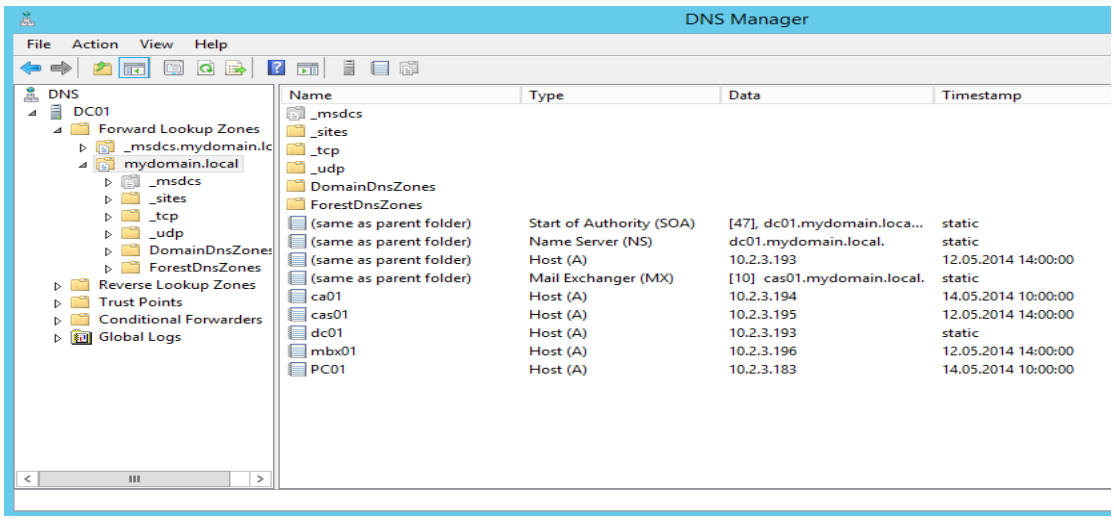
L'OU Client a été créé pour y mettre les comptes utilisateurs et machines régis par la GPO (plus bas).





9.3) Contenu DNS

On voit les différentes A et MX record enregistrées dans le DNS.

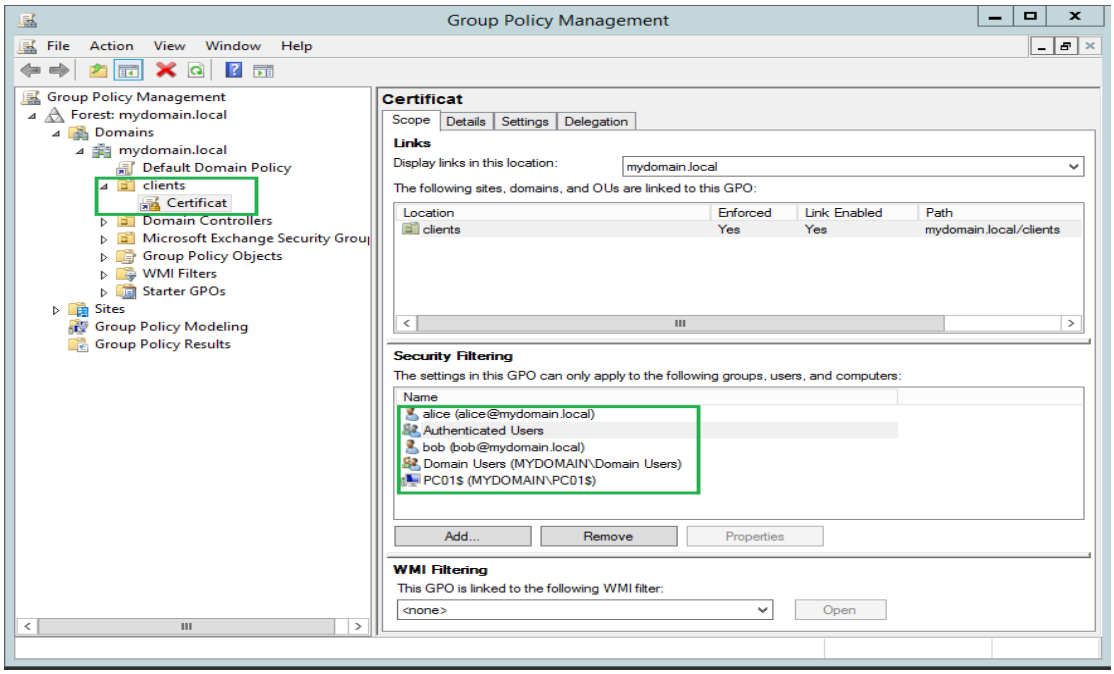


9.4) Contenu de la GPO

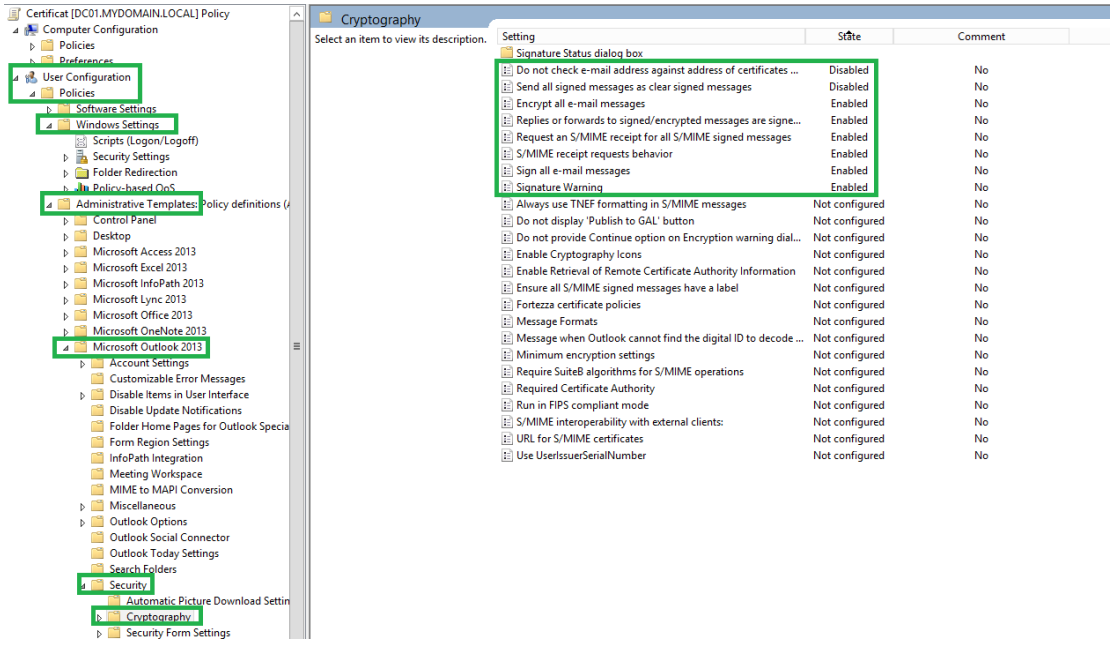
Cette GPO (Certificat) doit:

- transmettre le certificat de la CA aux clients
- affecter les comptes utilisateurs et machines
- permettre aux clients l'auto-enrôlement du certificat du modèle « mail signing »
- configurer le logiciel client Outlook 2013 pour signature, émission de confirmation de l'état du message (altéré ou non), et alerte si la signature est invalide.

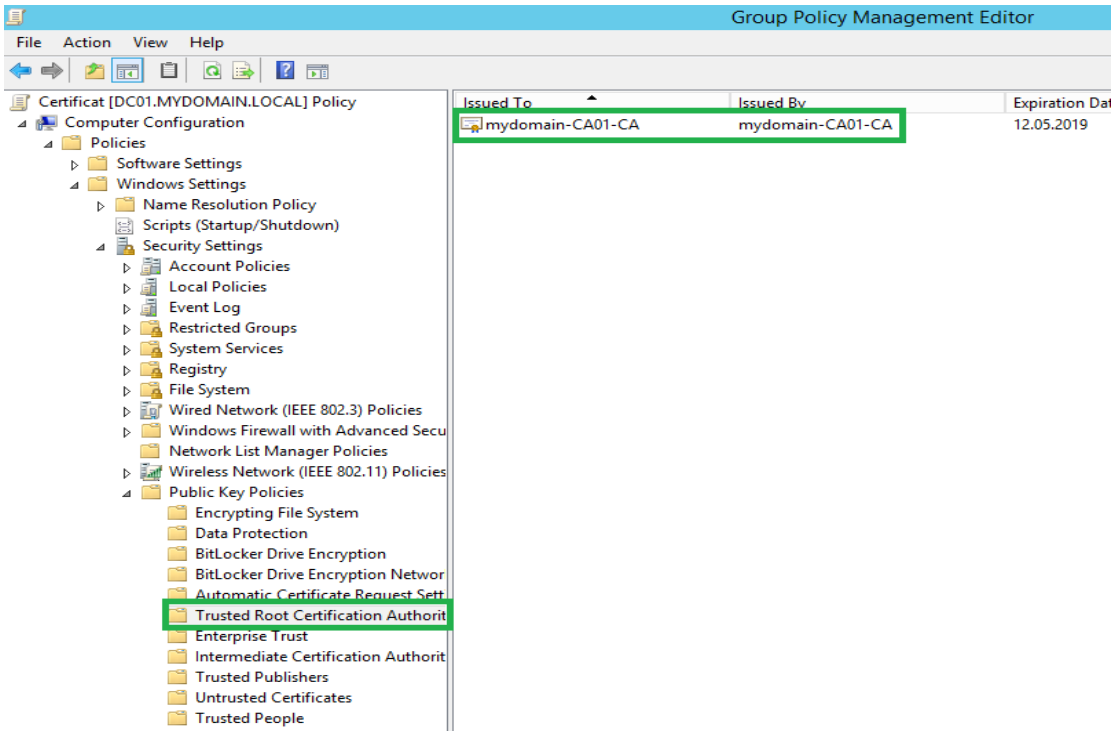
Affectation de la GPO



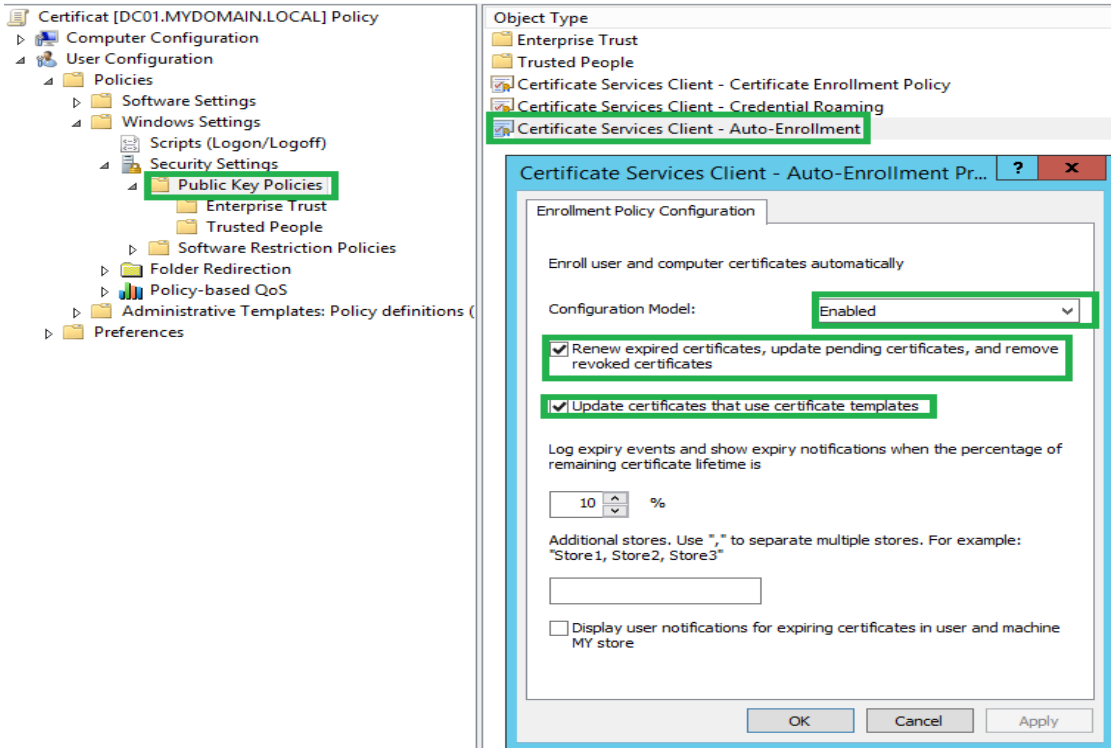
Configuration du logiciel Outlook par la GPO pour la signature et le chiffrement



Autorisation de la transmission du certificat de la CA à tous les clients



Autorisation de l'auto-enrôlement avec renouvellement automatique

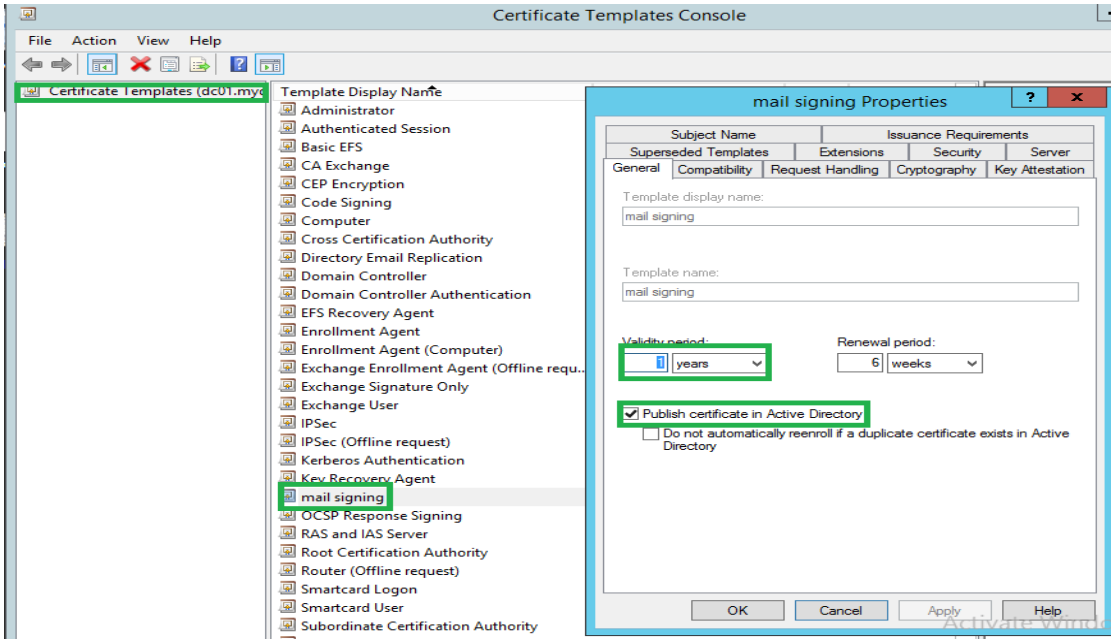


9.5) Configuration des modèles de certificats

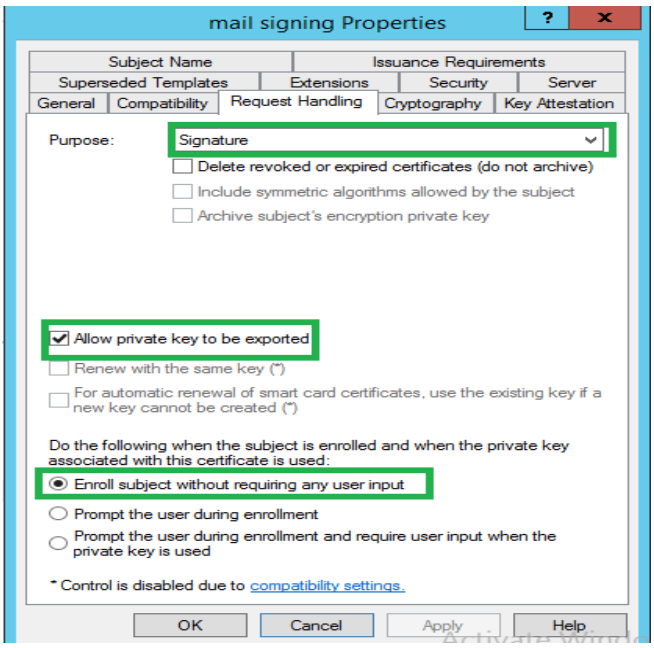
9.5.1) Modèle de la signature

Création du modèle de certificat : « mail signing » en dupliquant le modèle « User », avec les propriétés suivantes :

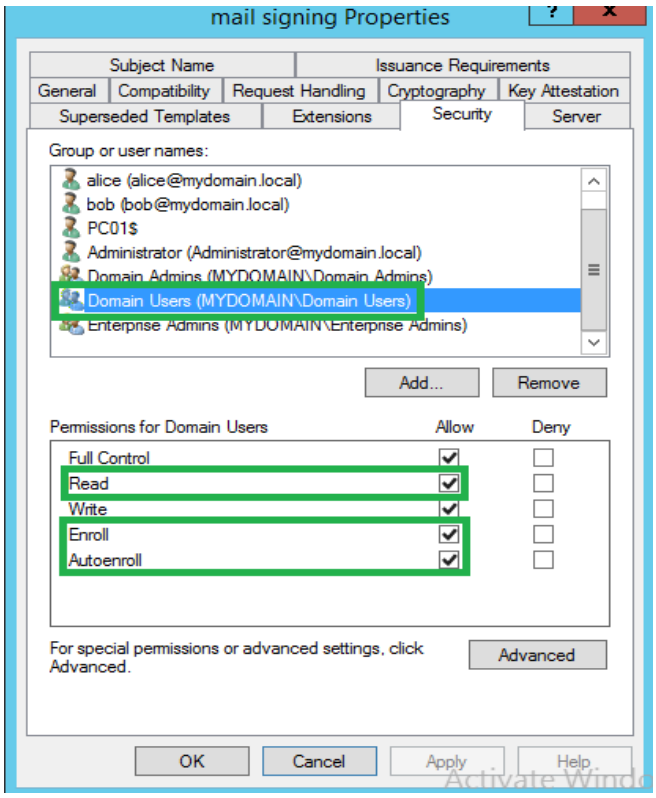
Le certificat sera valide 1 an et publié dans l'AD



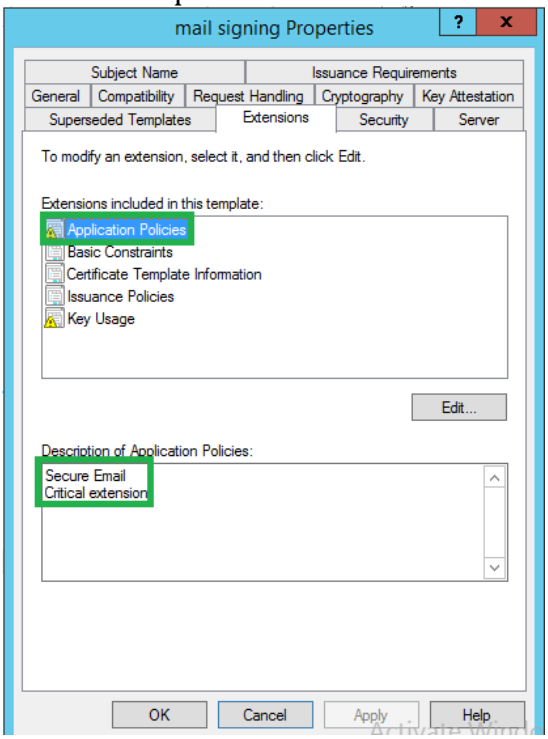
But du certificat : la signature, avec possibilité d'exporter la clef pour l'intégrer à un autre dispositif. L'utilisateur n'a besoin de donner aucune information lors de l'enrôlement.



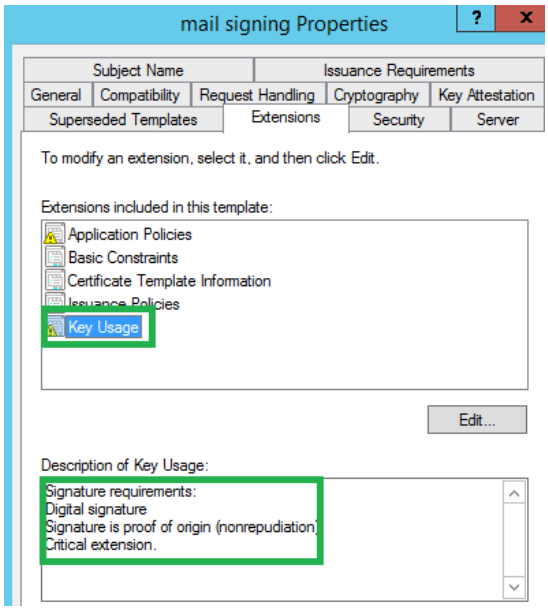
Pour permettre l'auto-enrôlement, il faut donner aux utilisateurs du domaine les autorisations suivantes :



Ce modèle a pour but la sécurité des mails



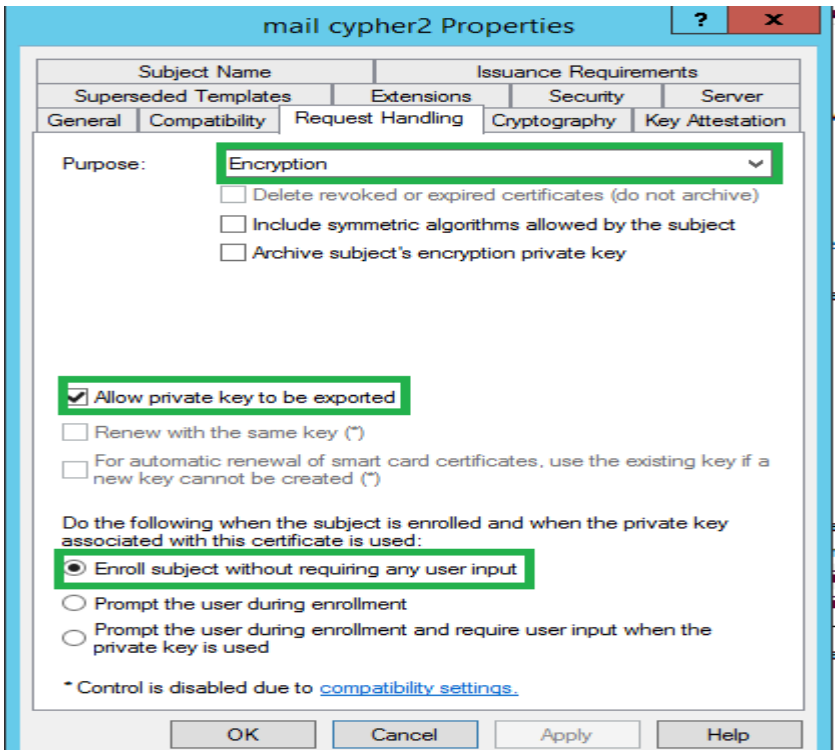
Certificat à utiliser à des fins de signature et de non-répudiation



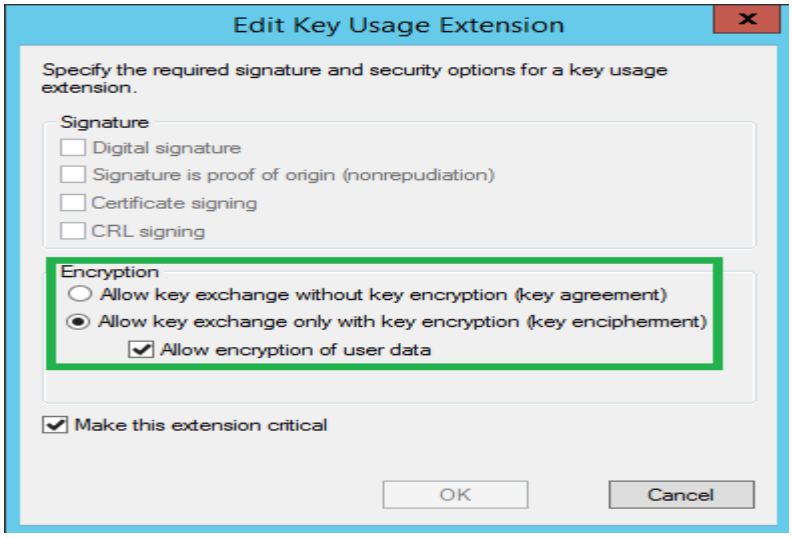
9.5.2) Modèle de chiffrement

Création du modèle de certificat : « mail cypher» en dupliquant le modèle « mail signing», avec les propriétés suivantes :

But du certificat : le chiffrement, avec possibilité d'exporter la clef pour l'intégrer à un autre dispositif. L'utilisateur n'a besoin de donner aucune information lors de l'enrôlement.



Le certificat sera utilisé à des fins de chiffrement



9.6) Microsoft Exchange

9.6.1) Choix du logiciel

Microsoft Exchange (existant en deux versions, standard et entreprise) est un logiciel serveur de messagerie très utilisé dans le monde entier par de nombreuses entreprises et organisations. La multiplication des plateformes Exchange dans le monde entier est due à la popularité croissante du «Hosted Exchange » dans le « Cloud » à bas prix (société OVH par exemple).
Il a été important de définir quelle version d'Exchange il serait préférable d'utiliser. Il ressort de l'analyse qu'il serait plus judicieux d'utiliser la version Exchange 2013 pour les raisons suivantes par rapport aux versions précédentes :

- Nombre de rôles moindres
- Outlook WebApp optimisée pour Smartphones, tablettes, PCs
- Protection contre la perte de données sensibles (DLP) grâce à une analyse de contenus

9.6.2) Versions

Microsoft Exchange 2013 est disponible en deux versions :

- Standard
- Entreprise

Les différences sont liées aux licences et sont expliquées dans la section suivante.

9.6.3) Licences

Pour faire fonctionner Exchange nous avons besoin de deux types de licences : les licences serveurs et les licences clients (CAL).

Licences serveurs :

Ces licences (Standard, Entreprise) permettent d'activer les fonctionnalités d'Exchange 2013 :

- La version standard est plutôt utilisée pour des petites et moyennes entreprises. Le nombre de bases de données de boîtes aux lettres supporté est compris entre 1 et 5.
- La version Entreprise, quant à elle, est plutôt destinée aux grandes organisations qui nécessitent un grand nombre de boîtes aux lettres et de bases de données de boîtes (jusqu'à 100).

Au final, la différence se situe au niveau du nombre de bases de données possibles. L'avantage d'avoir un grand nombre de bases de données de petite taille par rapport à un plus petit nombre de bases de données de boîtes de taille plus grande, est le temps de restauration des bases de données en cas de corruption, par exemple.
Une licence par processus Exchange est obligatoire, que ce soit dans un environnement physique ou virtuel.

Licences Clients (CAL) :

Ces licences permettent d'autoriser (de licencer) les connections des clients. Elles peuvent être « user based » ou « device based). Nous devons avoir autant de licences que d'utilisateurs ou de dispositifs. Le prix peut donc être exorbitant.
Il existe deux types de CAL avec des fonctionnalités bien différentes. En voici certains aspects :

Standard :

- *Sending and receiving e-mail and storing e-mails in a personal mailbox, and scheduling appointments and meetings and maintaining a personal calendar*
- *Browser-based access (via Outlook Web App) to e-mail, calendar, contacts, and tasks*
- *Built-in malware and spam filtering features of the Exchange software remove viruses, spyware, and unwanted messages from mail in transit*
- *Basic mobile device management, which enables mobile device access to Exchange via the Exchange ActiveSync protocol and covers synchronizing data with mobile devices and enforcing basic administrative policies such as minimum mobile device password length*

Entreprise :

- *Premium-level mobile device management, which enables more extensive policy enforcement via Exchange ActiveSync, such as the ability to prevent a mobile phone from being used as a modem for a PC*
- *Exchange Online Protection, a Microsoft-hosted service that filters e-mail going into or out of organizations for malware and spam and is available at no added cost to organizations that maintain Software Assurance coverage on the Exchange Enterprise CAL*
- *In-Place Archive (previously called Personal Archive), which provides organizations with a server-based e-mail archival option, that, unlike Outlook personal store (PST) files, can be reliably backed up by administrators, retained per corporate policy, and searched when necessary*
- *Data Loss Prevention, which analyzes message contents for sensitive information, such as personally identifiable information, and allows administrators to configure policies to filter messages or monitor the results.*[3]

Schéma montrant les différences entre les SCALs et ECALs :

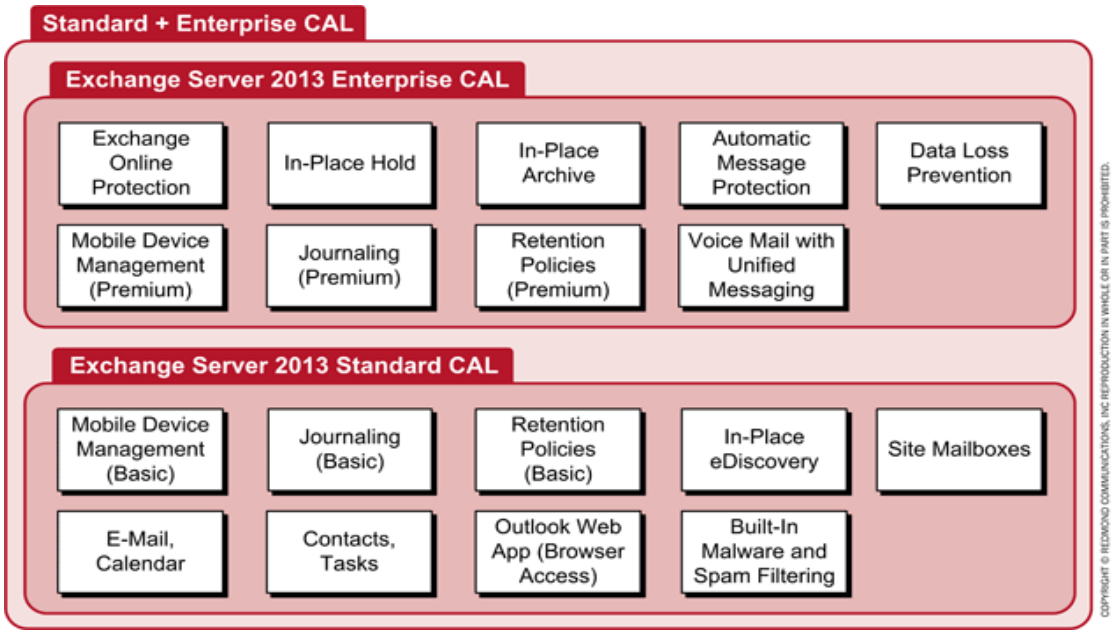


Figure 13 : Schéma récapitulatif[4]

[3] https://www.directionsonmicrosoft.com/licensing/2013/02/features-licensed-exchange-server-2013-cals
[4] https://www.directionsonmicrosoft.com/licensing/2013/02/features-licensed-exchange-server-2013-cals

Tableau récapitulatif des fonctionnalités, SCALs vs ECALs :

Feature	*Standard*	*Enterprise*
Email, calendar, contacts, and tasks	*Yes*	*Yes*
Outlook Web App (Internet Explorer, Firefox, Chrome, and Safari support)	*Yes*	*Yes*
Rich Outlook inbox experience, including enhanced conversation view and MailTips	*Yes*	*Yes*
Apps for Outlook and Outlook Web App	*Yes*	*Yes*
*Site mailboxes***	*Yes*	*Yes*
Role-based access control (RBAC) capabilities	*Yes*	*Yes*
Federated calendar sharing	*Yes*	*Yes*
Exchange ActiveSync mobile management policies	*Standard*	*Advanced*
Journaling	*Per database*	*Per user/distribution list*
Journal decryption	*No*	*Yes*
Unified Messaging	*No*	*Yes*
Retention policies	*Default*	*Custom*
*In-Place Archive***	*No*	*Yes*
Multi-mailbox search	*Yes*	*Yes*
In-Place Hold	*No*	*Yes*
*Data Loss Prevention (DLP)***	*No*	*Yes*
Information protection and control (IPC): transport protection rules, Outlook protection rules, Information Rights Management (IRM) search	*No*	*Yes*

Figure 14 : Tableau récapitulatif[5]

Les fonctionnalités offertes aux clients sont donc directement liées aux CALs et non par rapport aux licences du serveur. Un client qui voudrait bénéficier des fonctionnalités entreprises, doit s'acquitter d'une licence standard et d'une licence entreprise. C'est donc une licence supplémentaire.

9.6.4) Rôles dans Exchange 2013

Exchange 2013 ne possède que 2 rôles. Pour des raisons de sécurité notamment, il est conseillé de séparer les différents rôles fournis par Exchange sur deux serveurs physiques différents. En effet, nous ne donnons pas l'accès direct au serveur contenant les boîtes mails (« *Mailbox Server* »), mais nous passons par un système de redirection et de gestion des connexions (« *Client Access Server* »). Exchange 2013, contrairement à ses prédécesseurs, ne possède plus que 2 grands rôles au lieu de 5, dans cette architecture que nous pourrions qualifier de multi-rôles :

- Client Access Server (CAS)
- Mailbox Server (MBX)

[5] http://office.microsoft.com/en-us/exchange/microsoft-exchange-server-licensing-licensing-overview-FX103746915.aspx

9.6.4.1) Client Access Server rôle

Comme son nom l'indique, ce rôle sert d'intermédiaire entre le client et le Mailbox Server lors de connexions avec Outlook, OWA etc…

- Il est responsable d'authentifier, de fournir la connexion sécurisée SSL
- De rediriger et de router les différentes requêtes vers le bon Mailbox Serveur contenant la boîte mail de l'utilisateur.
- Il offre également les différents protocoles tels que le POP, SMTP, IMAP, RPC over HTTPS

Différents services sont assurés:

- Client Access Service : gère les connections entre les clients et la boîte mail
- Front End Transport Service : Fonction de filtrage des mails, routage de mails entre les serveurs Exchange et les serveurs externes.
- AutoDiscovery : Permet de configurer le client de messagerie (Outlook 2007 et plus) automatiquement en fonction des informations de logon si le client est dans un domaine

Il est possible d'avoir une redondance que l'on appelle Client Access array.

9.6.4.2) Mailbox Server

Ce rôle permet au serveur Exchange de :

- Stocker la base de données concernant les boîtes mails des clients
- Stocker les dossiers publics
- Responsable du stockage et du traitement des données
- Service Hub Transport permet le routage des mails dans l'organisation et la connexion entre le Front End Transport Service et le Mailbox Transport Service
- Service Mailbox Transport qui assure la connexion entre le Hub Transport Service et les bases de données de mails

Aucune connexion n'a lieu entre un client mail (Outlook, OWA…) et ce serveur et il ne doit pas être accessible depuis l'extérieur ou l'intérieur (excepté le CAS). Ce rôle est étroitement lié avec Active Directory, le Client Access Server et la base de données des boîte mails. Ce rôle peut également bénéficier d'une redondance en ayant plusieurs Mailbox Server formant un Database Availability Group (DAG).

9.6.4.3) Processus d'interaction entre rôles

1) The Mailbox server uses LDAP to access recipient, server, and organization configuration information from Active Directory.
2) The Client Access server sends requests from clients to the Mailbox server and returns data from the Mailbox server to the clients. The Client Access server also accesses online address book (OAB) files on the Mailbox server through NetBIOS file sharing. The Client Access server sends messages, free/busy data, client profile settings, and OAB data between the client and the Mailbox server.

3) Outlook clients inside your firewall access the Client Access server to send and retrieve messages. Outlook clients outside the firewall can access the Client Access server by using Outlook Anywhere (which uses the RPC over HTTP Proxy component).
4) Public folder mailboxes are accessible via RPC over HTTP, regardless of whether the client is outside or inside the firewall.
5) The administrator-only computer retrieves Active Directory topology information from the Microsoft Exchange Active Directory Topology service. It also retrieves email address policy information and address list information.

The Client Access server uses LDAP or Name Service Provider Interface (NSPI) to contact the Active Directory server and retrieve users' Active Directory information.[6]

Infrastructure et interactions entre les différents processus :

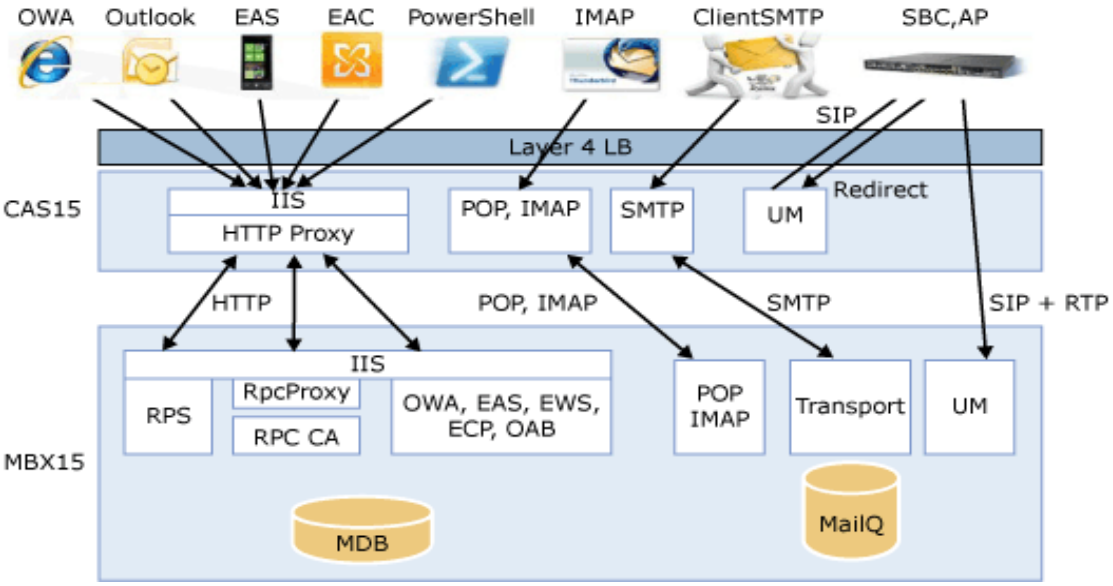


Figure 15 : Infrastructure et interactions entre les différents processus[7]

Voici les différents points importants que nous pouvons observer :

- Fonctionnalités du CAS :
  - IIS
  - HTTP / HTTPS Proxy ou redirection
  - Protocoles divers : POP, IMAP, SMTP
- Fonctionnalités du MBX :
  - IIS Server
  - OWA (Outlook Web Access)
  - OAB (Online Adresss Book)
  - EAS (Exchange Active Sync pour appareils mobiles)
  - MailBox Store

Il y a redirection non seulement des requêtes mais également de protocoles. Si un client fait une requête HTTPS à destination du CAS, alors la connexion entre le CAS et le MBX sera également de l'HTTPS.

[6] http://technet.microsoft.com/en-us/library/jj150491(v=exchg.150).aspx
[7] http://technet.microsoft.com/en-us/library/jj150491(v=exchg.150).aspx

Une requête client -> CAS en IMAP alors CAS->MBX en IMAP

Voici un exemple de flux de messagerie

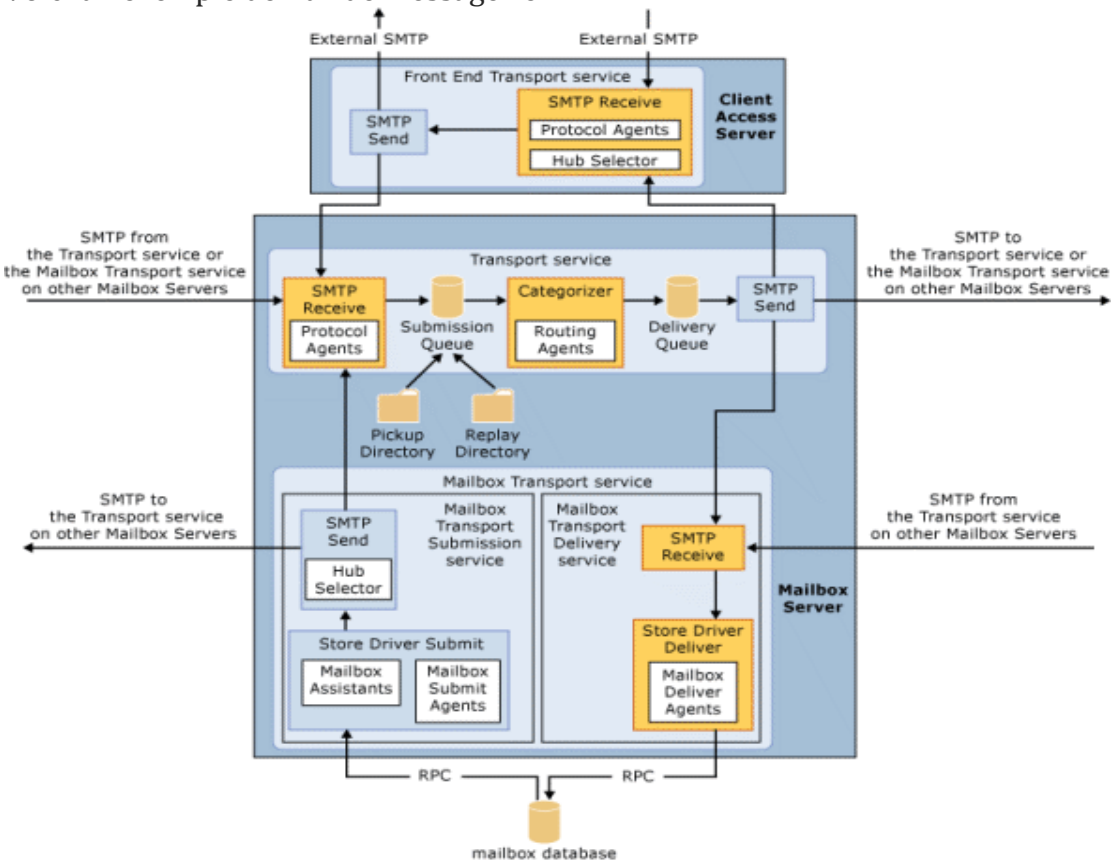


Figure 16 : Flux de messagerie[8]

9.7) PKI & Certificats

La gestion de la sécurité se fait par le Client Access Server. C'est à lui de fournir une connexion sécurisée SSL entre le serveur et le client (OutlookAnyWhere, Outlook, OWA…).
Nous avons bien sûr besoin de certificats pour assurer cette fonctionnalité (authentification des protagonistes, contrôle d'intégrité et confidentialité).

Par défaut Exchange installe, sur les Mailbox Servers et les Client Access Servers, un certificat auto-signé pour pouvoir chiffrer les communications concernant la messagerie entre eux. Etant donné que les clients ne se connectent jamais sur le Mailbox Server, il faudra faire en sorte qu'ils fassent confiance au certificat du Client Access Server uniquement.

On passe à une sécurité de couche applicative par la mise en service d'une PKI pour la gestion des certificats destinés à S/MIME (Secure/Multipurpose Internet Mail Extensions) pour la protection des mails.

8

On a donc utilisé un système de PKI afin de garantir la sécurité des mails échangés par les clients. Une telle infrastructure possède de nombreux avantages, mais également des inconvénients.

Avantages d'une PKI :

- Facilité de gestion
- Création, renouvellement suppression, invalidation de certificats aisés
- Grand choix d'algorithmes d'intégrité et de chiffrement
- Variété des tailles des clefs
- Prix faible

Inconvénients d'une PKI :

- Attention à la sécurité du certificat root de la PKI (clef privée)
- Certificat root inconnu des machines
- Nécessite l'installation du certificat root (clef publique) sur toutes les machines pour éviter les erreurs (Trusted Root Certificate Store)
- Attention à la gestion de la délivrance des certificats
- Attention à la règlementation en vigueur dans les pays concernant la taille des clefs.

9.8) Certificat Exchange

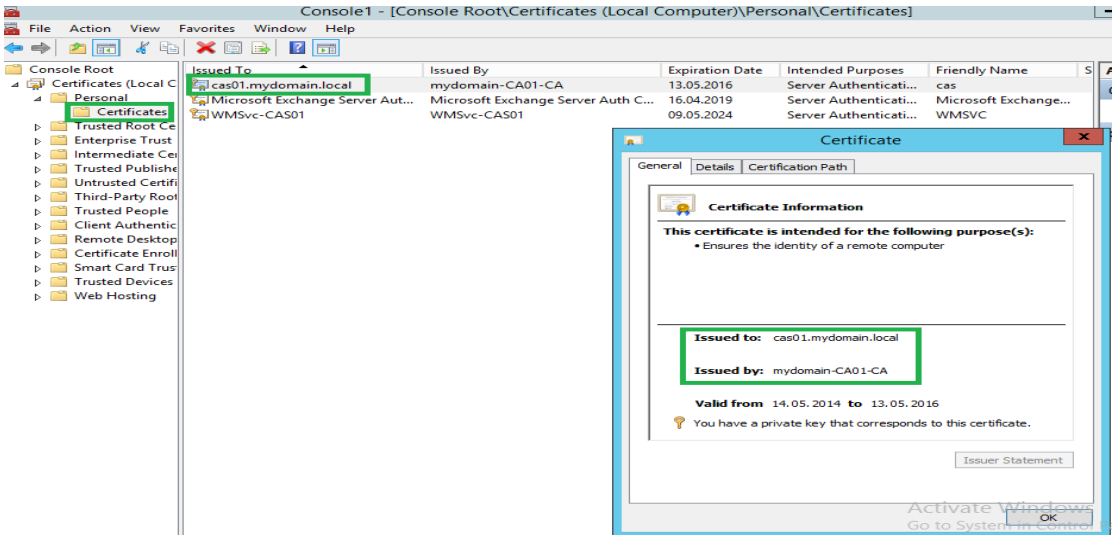


Figure 17 : Certificat CAS

Vérification de la présence du certificat après son installation
Sélection des services Exchange utilisant le certificat : aller dans la console d'administration d'Exchange et spécifier que le certificat sera utilisé pour les communications SMTP et HTTPS. Accessible via : https://cas01.mydomain.local/ecp

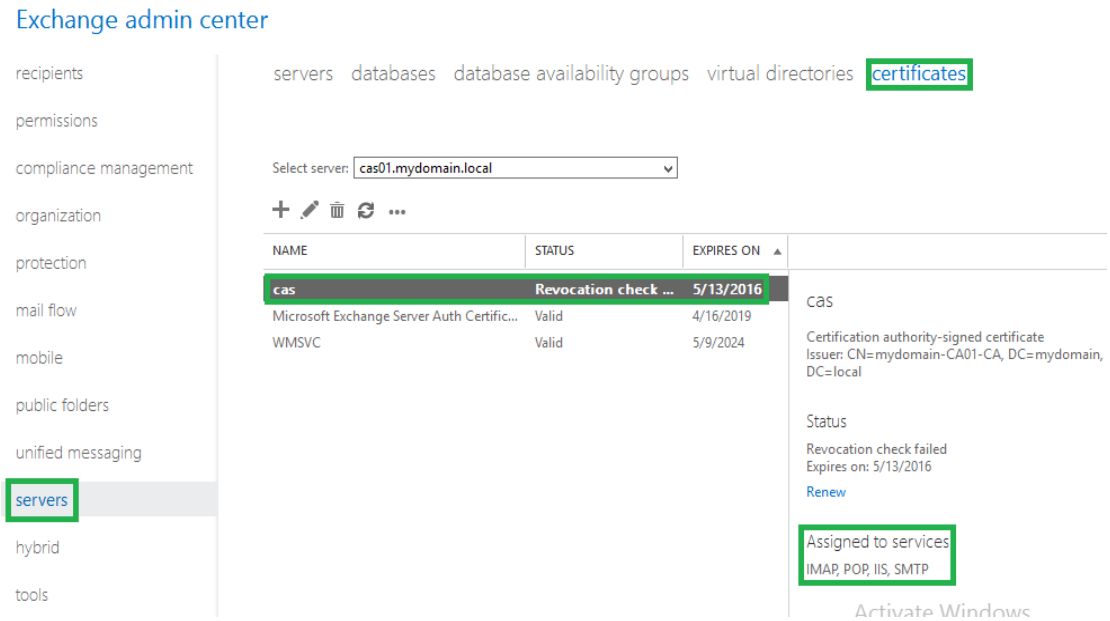


Figure 18 : Assignation des services

Une fois le certificat installé, toutes les connections concernant Exchange seront sécurisées.

9.9) Dual Key

La PKI fonctionne avec un système dit de « dual key », dans le scénario 1.c. En effet :

- Une clef est utilisée pour le chiffrement de données (archivable)
- L'autre pour la signature avec non-répudiation (non archivable)

Cela permet de spécifier :

- Des algorithmes de signature
- Des algorithmes de chiffrement différents
- Des périodes de validité différentes

Il est important de tenir compte du risque de perte de la clef privée de chiffrement rendant impossible le déchiffrement et donnant lieu à une perte de données.
Il est possible d'archiver la clef privée de chiffrement (mais non de signature), permettant ainsi de la récupérer pour le déchiffrement en cas de perte.
On peut également renouveler la clef privée pour le chiffrement sans perte de données, alors qu'en général la clef de signature doit être détruite lors d'une nouvelle demande.

9.10) Backup des clefs

Nous avons dans la CA, une possibilité de sauvegarder (archiver) les clefs privées et les certificats. Il existe deux procédures distinctes :

- L'archivage de la clef privée
- La sauvegarde des certificats

Ces deux éléments n'ont rien à voir ensemble au niveau procédural.

En ce qui concerne la signature :
En cas de perte de la clef privée ou si elle est compromise (avec risque de perte de l'intégrité et de la non-répudiation), il faut demander un nouveau certificat et révoquer l'ancien pour éviter que la clef soit utilisée. Aucune solution n'a été trouvée dans la CA pour archiver la clef privée pour la signature.

En ce qui concerne le chiffrement :
Ce cas est plus grave. La perte de la clef rend impossible le déchiffrement d'anciens mails, par exemple, et se traduit donc par la perte des données. Mais en suivant ces procédures, on peut archiver les clefs privées et les redonner aux clients, si nécessaire :
http://technet.microsoft.com/en-us/library/cc770588.aspx
http://technet.microsoft.com/en-us/library/cc753011.aspx
http://technet.microsoft.com/en-us/library/cc753826.aspx
http://technet.microsoft.com/en-us/library/cc733156.aspx

En ce qui concerne les certificats (pour les clefs publiques)
Nous pouvons exporter la base de données de la CA, pour la sauvegarder :
http://www.unitrends.com/documents/administrators-guide/user_manual/protecting_windows/certificate_services_database_backup_and_restore.htm
Sinon, il existe des scripts en C# et power Shell pour l'exportation dans un dossier.

Scénario 2

Internet

Emails signés & chiffrés

I/ Introduction

1.1) Contexte

Le but de ce projet est donc la mise en place d'une infrastructure de messagerie basée sur les produits Microsoft (Windows Server 2012 & Exchange 2013) avec la transmission de mails sur Internet. Ce travail se fera dans la salle de laboratoire de l'HEPIA afin de pouvoir effectuer les différentes installations des logiciels et systèmes d'exploitation, configurations et tests avant une éventuelle mise en production. Voici les scénarios :

- Scénario 2.a : réception de mails non sécurisée depuis Internet
- Scénario 2.b : envoi de mails non sécurisé vers Internet
- Scénario 2.c : envoi et réception de mails signés
- Scénario 2.d : envoi et réception de mails chiffrés

Une PKI sera mise en œuvre pour bénéficier des possibilités de non-répudiation, de contrôle d'intégrité et de chiffrement grâce à l'utilisation de certificats. La problématique de la sécurité (firewall, antivirus, anti-spam, sauvegarde, tolérance de pannes) ne sera pas traîtée ici.

1.2) Schéma

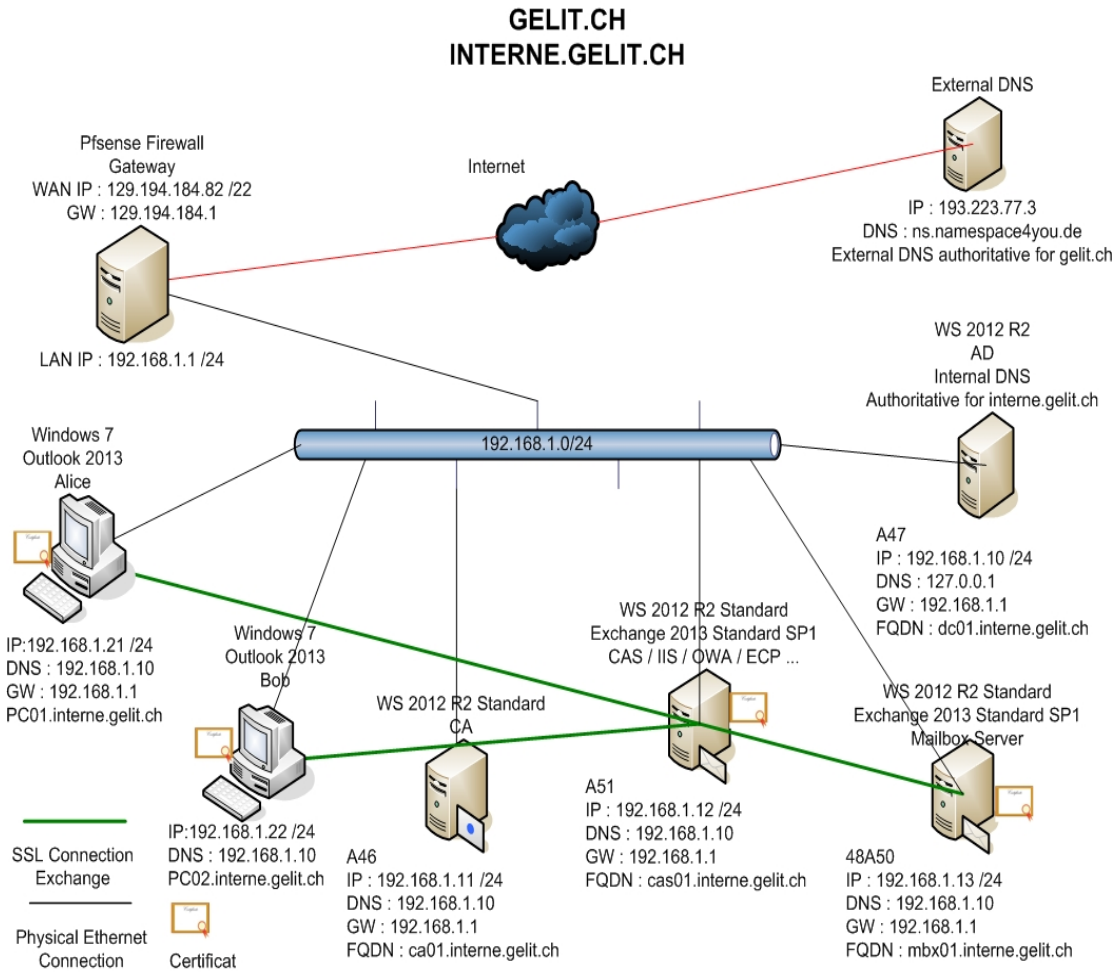


Figure 1 : Schéma de l'installation

1.3) Analyse

Dans cette partie, les points suivants sont traités :

- Connecteurs Exchange (flux SMTP) et connexions clients (flux HTTPS)
- Flux DNS
- Certificate Practice Statement
- Pare-feu pfSense (configuration en 2.3.4)
- ESMTP

1.3.1) Connecteurs Exchange et connexions clients

Il est important de déterminer le fonctionnement des différents connecteurs d'Exchange qui influent directement sur les flux des messageries de courrier entrant et sortant. Lors de l'installation d'Exchange, les connecteurs de réception sont créés automatiquement et configurés en mode permissif, afin de pouvoir recevoir des mails sans avoir à modifier la configuration par défaut. Cette configuration est à changer pour avoir un meilleur contrôle de ces flux. La règle d'or en matière de sécurité, est l'isolation du MBX. Personne ne doit pouvoir atteindre ce serveur à part le CAS. De plus, le MBX ne doit pas être utilisé pour l'envoi de mails. En effet, par défaut, le MBX est responsable de l'établissement des connexions SMTP et de la transmission des mails, ce qui n'est pas une bonne configuration. Les connecteurs seront configurés afin d'assurer cette isolation du MBX.

Pour permettre la réception des mails, il faut faire appel au *« receive connector »* pour le CAS ainsi que le MBX.

Pour le CAS, il existe 3 connecteurs par défaut, indépendants les uns des autres :

1) Default FrontEnd CAS01 : permet les connexions SMTP des autres serveurs
2) Outbound Proxy Frontend CAS01 : accepte les messages des serveurs back-end (MBX01) possédant un connecteur d'envoi, utilisant un proxy
3) Client Frontend CAS01 : accepte les connexions sécurisées TLS avec des partenaires de messagerie spécifique

- En ce qui concerne le premier connecteur, c'est un fondamental pour permettre la bonne réception des mails par SMTP en provenance des serveurs de messagerie publique. Il n'y a pas grand chose à changer.
- Pour le deuxième connecteur, il y a quelques changements à effectuer, afin de s'assurer que seul le MBX01 soit en mesure de se connecter au CAS en se servant de lui comme proxy de messagerie. Il ne doit être activé et configuré que si nous voulons que le MBX passe par le CAS.
- Le troisième connecteur permet de choisir une configuration spécifique (autorisations IPs, permissions…) avec un partenaire de messagerie

Pour le MBX, il existe 2 connecteurs par défaut :

1) Default MBX01 : accepte les connexions provenant des MBX possédant un rôle de transport et des serveurs Edge
2) Client Proxy MBX01 : accepte les connexions des serveurs FrontEnd

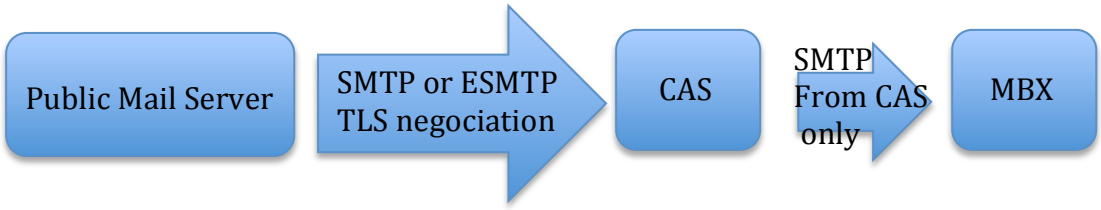
- Le premier connecteur ne sert donc qu'à la communication entre différents MBX qui seraient présents dans l'infrastructure.
- Le deuxième connecteur n'est utile que s'il y a un serveur avec un rôle FrontEnd en DMZ

Etant donné qu'il n'y a qu'un seul MBX et pas de FrontEnd, ces deux connecteurs ne sont pas utiles. Pour des raisons de sécurité, un nouveau connecteur sera créé et configuré afin que seul le CAS puisse communiquer avec lui. Il faut absolument que le MBX soit isolé et ne soit accessible que par le CAS.

Pour permettre l'émission de mails, il faut faire appel au *« send connector »* (présent sur le MBX).
Par défaut, c'est le serveur possédant le rôle de transport (ici le MBX) qui émet les mails vers un serveur de messagerie de destination, ce qui n'est pas une configuration correcte. Pour des raisons de sécurité et afin de garantir l'isolation du MBX, il est préférable de le « cacher » derrière le CAS. La connexion SMTP se fera par le CAS. C'est ici que le connecteur de réception « Outbound Proxy FronteEnd CAS01 » est important. Il configure et autorise l'utilisation du CAS comme proxy pour le MBX.

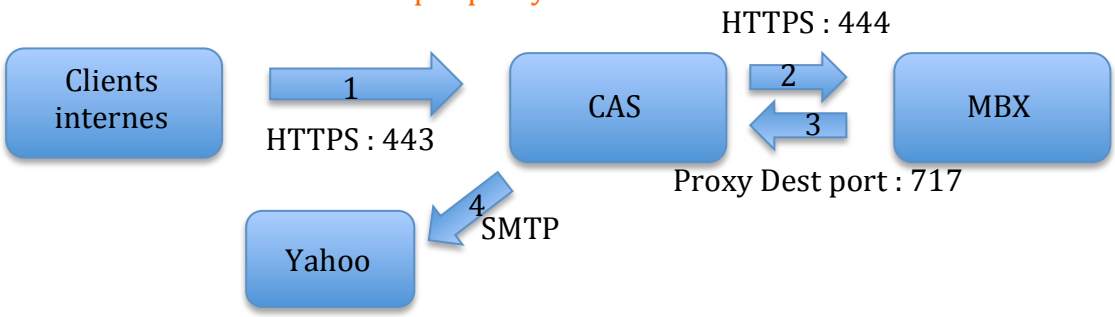
En ce qui concerne les clients, avec Exchange 2013, les connexions se font uniquement par Outlook Anywhere (RPC over HTTPS). Toutes les connexions des clients (Outlook, OWA, Smartphone…) se font par le biais de HTTPS avec IIS uniquement, ce qui réduit considérablement le nombre de ports utilisés.

Flux SMTP de réception à obtenir



Flux SMTP et HTTPS par défaut en émission :

Flux SMTP et HTTPS de mails par proxy en émission :

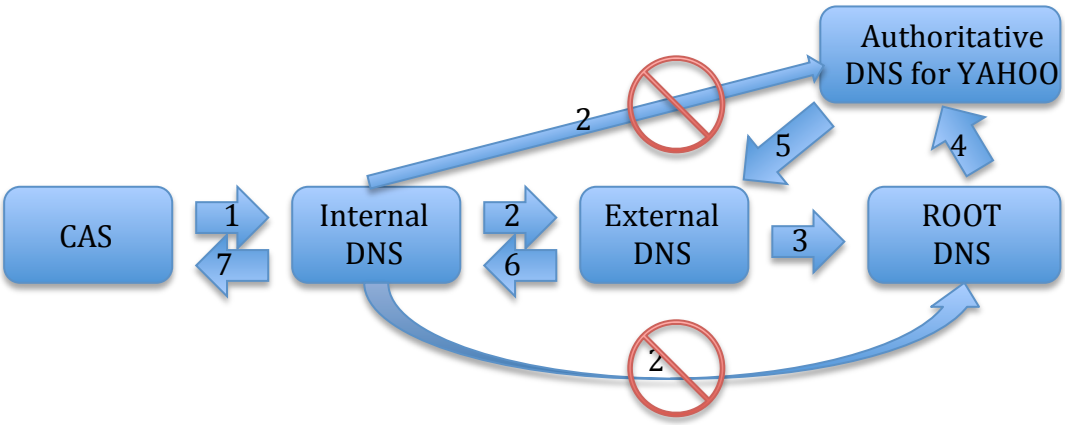


1.3.2) Flux DNS

Comme le montre le schéma principal, on utilise deux serveurs DNS. En effet, j'utilise la notion de sous-domaine (pas de split DNS ou de domaine interne privé en local). Le fait d'avoir deux serveurs DNS, offre une sécurité supplémentaire, chacun de ces serveurs ayant un rôle spécifique.

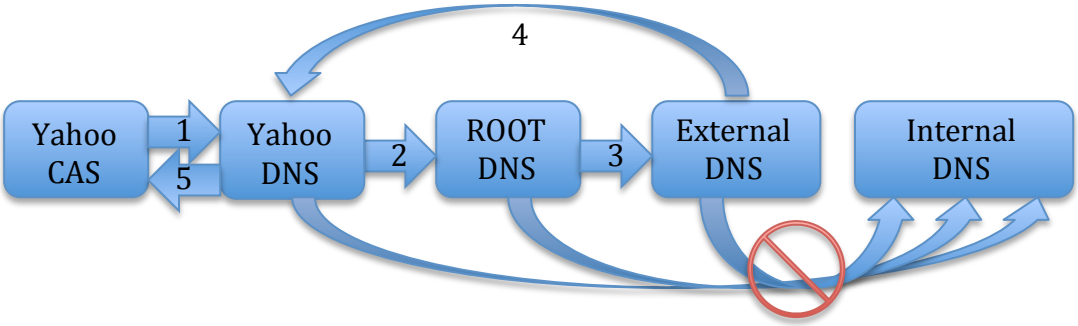
- Le serveur DNS interne ne s'occupe que des requêtes DNS en interne et n'est autoritaire que pour le sous-domaine (interne.gelit.ch). Il répond aux requêtes DNS adressées à interne.gelit.ch par les postes clients internes, les serveurs de messageries Exchange et aux recherches des objets dans l'AD. Il n'est pas accessible depuis l'extérieur.
- Le serveur DNS public répond aux requêtes adressées à gelit.ch par les clients Outlook externes et les serveurs de messagerie publics. Pour des raisons de sécurité, ce serveur sert également pour atteindre un serveur de messagerie externe lorsque le CAS a besoin d'effectuer une résolution DNS,. Le serveur DNS interne ne fait que relayer la demande au serveur public
- *http://acbrownit.wordpress.com/2013/04/15/active-directory-domain-naming-in-the-modern-age/*

Flux DNS simplifié pour l'émission de mails (gelit→yahoo)



1) MX of yahoo.com ? asking internal DNS
2) Not in cache, asking External DNS
3) Not in cache, asking ROOT DNS
4) Not in cache of Root DNS (MX Found in the Yahoo DNS)
5) Transmitting MX from Authoritative DNS for Yahoo to external DNS
6) Transmitting MX from external DNS to internal DNS
7) Transmitting MX from internal DNS to CAS

Flux DNS simplifié pour la réception de mails (yahoo→gelit)



1) Mail server of yahoo asking for MX of gelit.ch to its DNS Server
2) Yahoo DNS server asking to Root DNS
3) Root DNS asking to authoritative DNS server of gelit.ch
4) Transmitting MX from Authoritative DNS for gelit to Yahoo DNS
5) MX transmitted to Yahoo mail server

1.3.3) Certificate Practice Statement

Le CPS est un document provenant d'une autorité de certification qui décrit les règles pour la délivrance et la gestion des certificats.
Il est important de pouvoir mettre en place un CPS suivant les besoins de sécurité de l'organisation. Pour arriver à un CPS, il faut passer par une Security Policy (SP) et des Certificate Policies (CPs).

Le CPS est la mise en pratique d'une SP et d'un CP :

- Identité de la CA
  - interne.gelit-CA01-CA
- Type de certificat délivré
  - Mail signing
- Procédure pour la délivrance, le renouvellement et le recouvrement des certificats
- Durée des certificats
  - 1 an pour l'utilisateur
- Algorithme, CSP et longueur des clefs
  - Microsoft Enhanced Cryptographic provider, 2048 bits

Politique de révocation et de distribution des CRLs

La SP est un document qui définit les différentes règles d'utilisation des services de sécurité. Les questions qui se posent sont les suivantes:

- Quelle application est sécurisée par ces certificats ?
  - Service de messagerie
- Quels types de services assurent ces certificats ?
  - Protection des mails, signature / non-répudiation

La CP, quant à elle, s'occupe des certificats et est responsable de la CA. Caractéristiques principales :

- Qui peut s'enrôler ?
  - Les membres des communes-réunies
- Informations nécessaires pour l'enrôlement et le renouvellement :
  - Nom, âge, fonction, organisation, département, commune, email

- Comment est authentifié l'utilisateur lors de l'enrôlement ?
- Procédure de délivrance des certificats :
    - Déplacement du client vers le lieu de délivrance, vérification d'une pièce d'identité, de la fonction dans l'organisation ainsi que de l'email, signature d'un contrat, stockage des clefs sur une clef USB
- Management des clefs privées
    - Aucun archivage
    - Clefs non exportables
    - Une clef par utilisateur
- Utilisation (but du certificat)
    - Signature des mails et non-répudiation
- Taille des clefs
    - 2048 bits RSA
- Procédure en cas de perte de la clef par l'utilisateur

1.3.4) Pare-feu

Etant donné que les serveurs ont une connexion Internet, ils sont exposés aux menaces. Il est important de sécuriser l'infrastructure à l'aide de pfSense (en défense périmétrique). Des règles de pare-feu et de NAT sont mises en place afin de limiter les communications strictement au CAS et de bloquer le trafic entrant/sortant du MBX pour en garantir l'isolation. Le flux DNS du DNS interne est également autorisé.
La configuration se trouve plus loin dans le rapport (2.3.4).

1.3.5) ESTMP

Il existe une version étendue du protocole SMTP appelée ESMTP. Ce protocole utilisé par les serveurs de messageries facilite la mise en place de la sécurité et l'installation de la configuration.
On sait que pour des raisons de sécurité une version SSL de SMTP (SMTPS) a été développée il y a quelques années. L'inconvénient de cette solution c'est qu'il faut utiliser des ports différents (465 au lieu de 25). ESMTP remédie à cela en donnant accès à une nouvelle commande : STARTTLS, pouvant donner lieu à une communication chiffrée sur le port 25. Si un des serveurs ne supporte pas STARTTLS, on retourne à une connexion en clair.

Lors d'une connexion SMTP, les serveurs de messageries se transmettent diverses commandes. L'émetteur peut envoyer une commande EHLO au lieu de HELO, afin d'exprimer la volonté d'utiliser ESMTP. Si les 2 serveurs se mettent d'accord sur ESMTP, ils ont accès à des commandes supplémentaires telles que :

- AUTH : qui permet d'authentifier un client se connectant au serveur
- STARTTLS qui commande la mise à niveau des connexions en clair, en connexions sécurisées (SSL/TLS) sur le port 25.

Exchange 2013, supporte pleinement STARTTLS et peut négocier l'échange des clefs et le chiffrement des communications.

II/ Scénario 2.a (réception de mails)

2.1) Cahier des charges

Les différents services, logiciels, matériels et autres prérequis pour la mise en place d'une messagerie dans le cadre de ce projet sont les suivants:

- Un nom de domaine public mis à disposition = gelit.ch
- Un nom de sous-domaine privé interne : interne.gelit.ch
- Un serveur et une zone DNS publics
- Un serveur et une zone DNS privés isolés en interne
- Un serveur Active directory (DC01.interne.gelit.ch)
- Un enregistrement des records A des serveurs et postes clients (automatique pour les membres du domaine, DNS interne) et MX (manuel pour le serveur Exchange, DNS interne et externe)
- Un Mailbox Server (Exchange Server 2013 SP1) (MBX01.interne.gelit.ch)
- Un Client Access Server (idem) (CAS01.interne.gelit.ch)
- Windows Server 2012 Standard pour tous les serveurs
- 2 postes clients membres du domaine avec Windows 7 et Outlook 2013

2.2) Etapes d'installation

Les étapes d'installation sont celles du 2.4 du Scénario 1 pour les détails et les précisions. Seules les différences sont indiquées ici.

2.2.1) Configuration AD

Eléments de configuration AD :

- Création d'une nouvelle forêt
- Root Domain Name : interne.gelit.ch
- Forest Fonctional Level : Windows Server 2012 R2
- Domain Fonctional Level : Windows Server 2012 R2
- Ajout de ce domaine dans le DNS (Création du DNS automatique)
- Ce serveur est un GC
- Mot de passe DSRM : HEpia10
- NetBIOS name : GELIT

2.2.2) Configuration DNS

Les Microsoft best practices recommandent d'utiliser un sous-domaine plutôt que des extensions de type .local, .privé… Cela se traduit par la gestion de deux domaines, mais reste plus sûr.
http://www.mdmarra.com/2012/11/why-you-shouldnt-use-local-in-your.html
http://acbrownit.wordpress.com/2013/04/15/active-directory-domain-naming-in-the-modern-age/

2.2.2.1) DNS Externe (ns.namespace4you.de)

Ce serveur DNS est important afin que les hôtes externes puissent localiser notre serveur CAS. Il faut donc ajouter sur le serveur DNS des records A et MX.

- A record : mail.gelit.ch, type = A, Data = 129.194.184.82
- MX record : name : gelit.ch, type = Mx, Data : [10] mail.gelit.ch

2.2.2.2) DNS Interne (dc01.interne.gelit.ch)

Etant donné que nous avons une configuration automatique, avec une zone DNS de type AD Integrated, par défaut, les records A des ordinateurs (membres du domaine uniquement) sont dynamiquement insérés dans la base.
Nous n'avons qu'une entrée à rajouter dans la zone interne.gelit.ch, un record MX pointant sur le CAS pour la localisation du serveur par les clients internes :

- MX Record : name : (same as parent folder), type = Mx, Data : [10] cas01.interne.gelit.ch

2.2.3) Configuration Exchange

2.2.3.1) Configuration des utilisateurs

Lorsqu'un utilisateur est créé, il possède une adresse par défaut, telle que : alice@interne.gelit.ch, le domaine Windows actuel étant : interne.gelit.ch. Pour que l'utilisateur puisse envoyer et recevoir des mails avec le nom de domaine public : gelit.ch (alice@gelit.ch) il faut :

1. Rendre le serveur Exchange autoritaire pour le domaine gelit.ch
2. Rajouter à l'utilisateur une adresse SMTP prenant le nom de domaine public comme domaine

Pour l'étape 1, veuillez suivre la procédure :
http://www.techieshelp.com/exchange-2013-setup-accepted-domains/
Valeur à insérer pour les deux champs : gelit.ch, de type *« Authoritative domain »*

Pour l'étape 2, veuillez suivre la procédure:
http://technet.microsoft.com/en-us/library/bb123794(v=exchg.150).aspx
Adresse SMTP à rajouter de type username@gelit.ch

Cette étape peut être automatisée par le biais des *« email address policies »*
http://technet.microsoft.com/en-us/library/bb125137(v=exchg.150).aspx
On peut spécifier que tous les utilisateurs auront gelit.ch comme domaine principal dans leurs mails.

2.2.3.2) Configuration réception des mails

Procédure :http://www.techieshelp.com/setup-exchange-2013-receive-connector/

Eléments de configuration importants pour les connecteurs à modifier (CAS) :

Connecteur 1 : Default FrontEnd CAS01

- Sécurité
  - Authentification : TLS (permet de chiffrer la connexion entre serveurs SMTP grâce à ESMTP)
    - Concerne les connexions : Serveurs mail publics –-> CAS
  - Permissions : Anonymous Users (tous les serveurs SMTP peuvent s'y connecter)
- Scoping :
  - Remote network settings : IPv4 : 0.0.0.0-255.255.255.255 et IPv6 : ::-ffff :ffff :ffff :ffff :ffff :ffff :ffff :ffff (permet de recevoir les mails de n'importe quel serveur SMTP)
  - Network adapter bindings : 192.168.1.12 :25 (permet de lier cette configuration à cette IP (CAS01))

Connecteur 2 : Outbound Proxy Frontend CAS01

- Sécurité
  - Authentification: TLS (authentification mutuelle), Exchange server authentification
    - Concerne les connexions : CAS - MBX
  - Permissions : Exchange servers
- Scoping :
  - Remote network settings : 192.168.1.13 (accepte les connexions provenant du MBX01)
  - Network adapter bindings : 192.168.1.12 :717 (permet de lier cette configuration à cette IP (CAS01))
  - FQDN transmis lors de HELO/EHLO : cas01.interne.gelit.ch

Connecteur 3 : Client Frontend CAS01

- N'est pas utilisé ici. Pas de connexion sécurisée TLS avec un partenaire spécifique

Annexe 11.1)

Connecteur de réception pour le MBX

Voici la configuration d'un nouveau connecteur :

Nom : Receiver

- Sécurité
  - Authentification: TLS (mutual authentification), Exchange server authentification
  - Permissions : Exchange servers
- Scoping :
  - Remote network settings : 192.168.1.12-192.168.1.13 (accepte les connexions de lui-même et du CAS)
  - Network adapter bindings : 192.168.1.13 :25 (permet de lier cette configuration à cette IP (MBX01))
- FQDN transmis lors de HELO/EHLO: mbx01.interne.gelit.ch

2.2.4) Configuration pfSense

Règles de pare-feu et de NAT :
Afin d'assurer une sécurité maximale :

- toutes les connexions entrantes et sortantes sont bloquées
- Pour le DNS interne :
  - les requêtes DNS sortantes du DNS interne sont autorisées
- Pour le CAS
  - Le trafic entrant/sortant HTTPS et SMTP est autorisé
- Pour le MBX
  - Tout le trafic entrant/sortant est bloqué
- Les flux SMTP et HTTPS en provenance de l'extérieur sont redirigés vers le CAS

Configuration des règles (interface WAN)

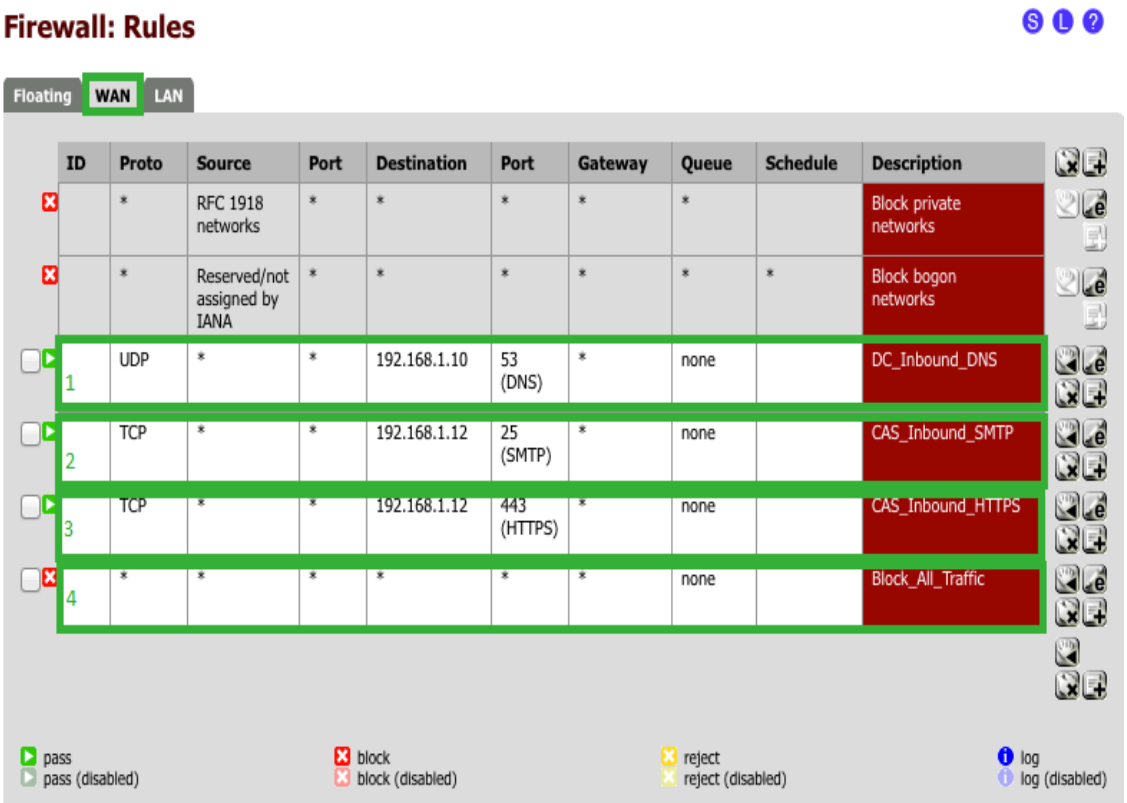


Figure 2 : Configuration règles WAN

1) Autorise le trafic DNS entrant vers le DNS interne (seulement en réponse à une requête sortante précédente)
2) Autorise tout le trafic SMTP entrant à destination du CAS
3) Autorise tout le trafic HTTPS entrant à destination du CAS
4) Tout le trafic restant est bloqué

Configuration du NAT

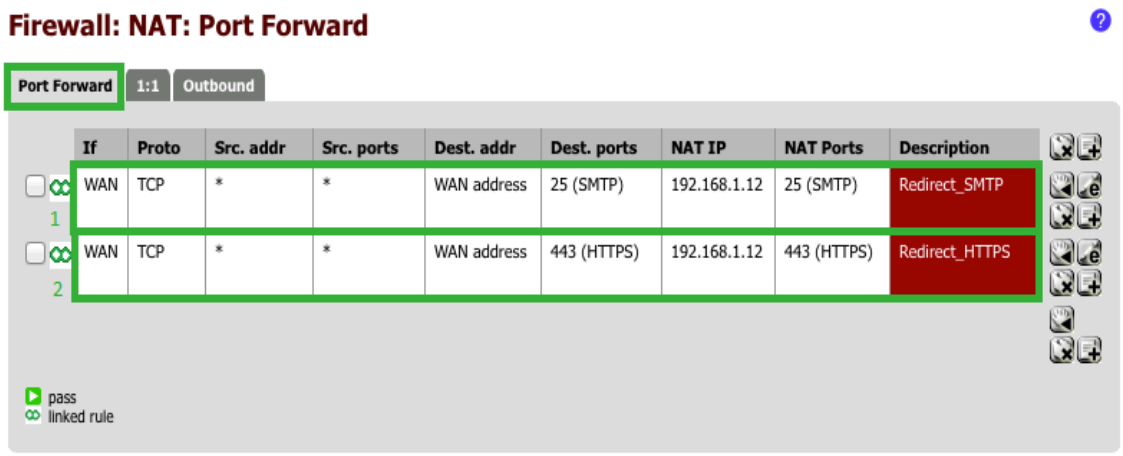


Figure 3 : Configuration NAT

1) Redirection du trafic SMTP entrant vers le CAS
2) Redirection du trafic HTTPS entrant vers le CAS

Configuration des règles (interface LAN)

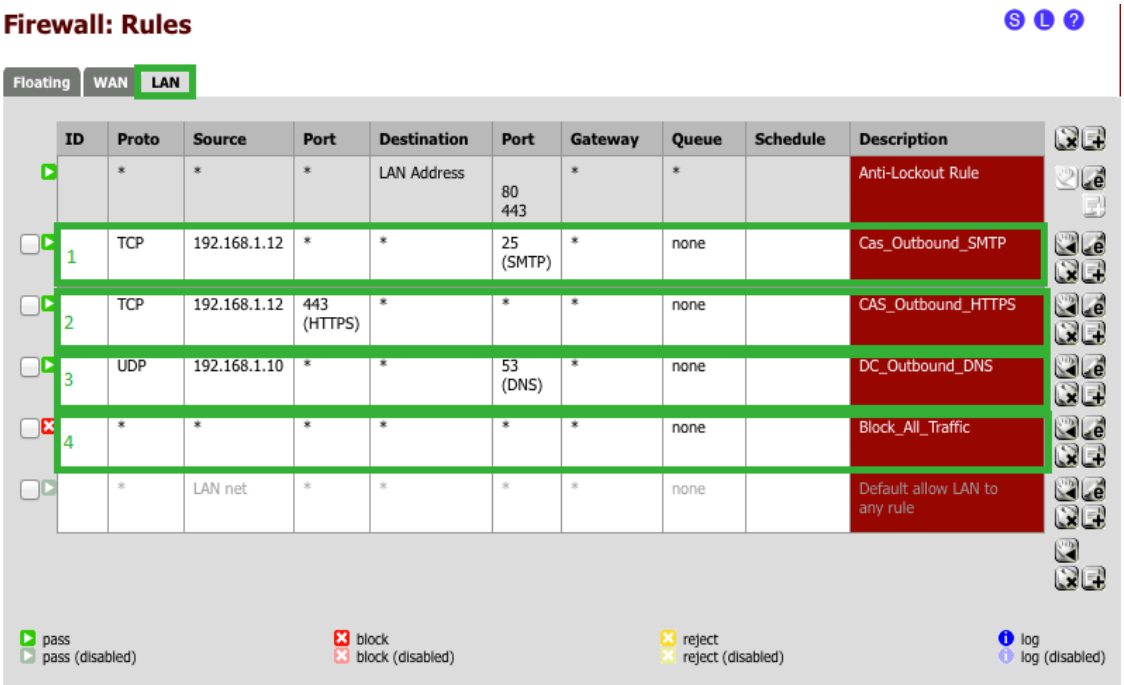


Figure 4 : Configuration règles LAN

1) Autorise le trafic SMTP sortant du CAS
2) Autorise le trafic HTTPS sortant du CAS (réponse à une requête entrante)
3) Autorise le trafic DNS sortant du DNS interne (DC01)
4) Tout le trafic restant est bloqué

III/ Tests Scénario 2.a (réception de mails)

Dans ce test, un mail est envoyé de jardonnour@yahoo.fr à destination de alice@gelit.ch.

Je vais montrer ici :

- Le header du mail
- Une capture Wireshark

Le mail est bien arrivé à alice@gelit.ch

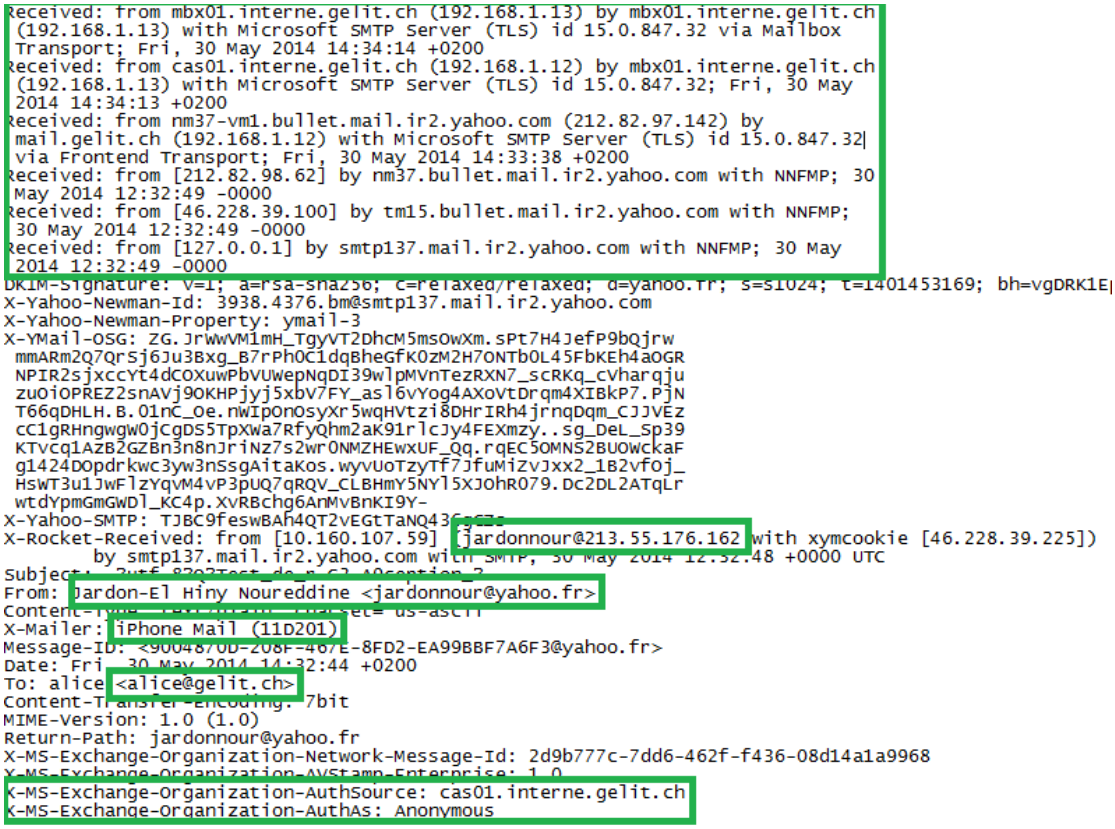


Figure 5 : Contenu du header du mail

Dans les encadrés en vert, on a les différents éléments importants contenus dans le header :

- Chemin du mail
- IP de l'émetteur
- Adresse de source
- Système source : iPhone
- Adresse de destination
- Serveur qui a authentifié la connexion : CAS01
- Données d'identification : anonymous

Tableau de routage du mail :

Hop	Delay	From	To	With	Time (UTC)
1	*	127.0.0.1	smtp137.mail.ir2.yahoo.com	NNFMP	5/30/2014 12:32:49 PM
2	0 sec	46.228.39.100	tm15.bullet.mail.ir2.yahoo.com	NNFMP	5/30/2014 12:32:49 PM
3	0 sec	212.82.98.62	nm37.bullet.mail.ir2.yahoo.com	NNFMP	5/30/2014 12:32:49 PM
4	49 sec	nm37-vm1.bullet.mail.ir2.yahoo.com 212.82.97.142	mail.gelit.ch 192.168.1.12	Microsoft SMTP Server (TLS)	5/30/2014 12:33:38 PM
5	35 sec	cas01.interne.gelit.ch 192.168.1.12	mbx01.interne.gelit.ch 192.168.1.13	Microsoft SMTP Server (TLS)	5/30/2014 12:34:13 PM
6	1 Sec	mbx01.interne.gelit.ch 192.168.1.13	mbx01.interne.gelit.ch 192.168.1.13	Microsoft SMTP Server (TLS)	5/30/2014 12:34:14 PM

Figure 6: Routage du mail

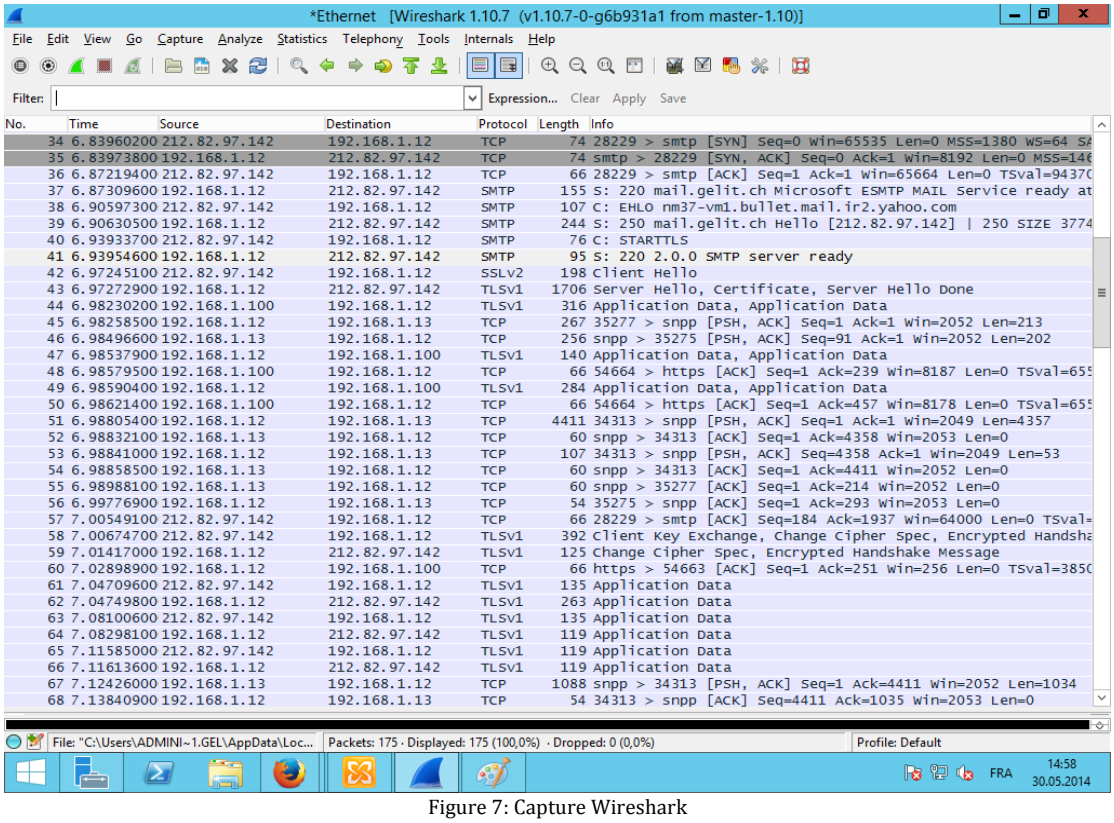


Figure 7: Capture Wireshark

Dans cette analyse Wireshark on a :

- La demande de connexion du serveur Yahoo au CAS01 (SYN, ACK…)
- Le Message EHLO (Permet l'utilisation de ESMTP qui donne accès à TLS)
- L'échange de clef pour la connexion TLS (client key exchange)
- L'échange de données du mail chiffré TLS (application data)

IV/ Scénario 2.b (envoi de mails)

4.1) Configuration Exchange

L'important, dans cette partie, c'est de configurer un *« send connectors »*.

Procédure :
http://www.techieshelp.com/exchange-2013-send-connector-configuration/

Eléments de configuration à remplacer :
- Nom : External
- Utiliser les MX records
- Domaine : * (afin de pouvoir envoyer à tous les domaines)
- Serveur de source : MBX01

Une fois le connecteur créé, il faut encore le modifier :
- Dans l'onglet général : cocher le *« Proxy through CAS »*
- Dans Scoping : FQDN : mail.gelit.ch

Annexe 11.2)

V/ Tests Scénario 2.b (envoi de mails)

Dans ce test, un mail est envoyé de alice@gelit.ch à jardonnour@yahoo.fr

Voici :

- Le header du mail
- Une capture Wireshark de SMTP uniquement due à trop d'informations

Le mail est bien arrivé à jardonnour@yahoo.fr

```
X-Apparently-To: jardonnour@yahoo.fr via 46.228.37.143; Fri, 30 May 2014 14:16:45 +0000\
Return-Path: <alice@gelit.ch>\
Received-Spf: none (domain of gelit.ch does not designate permitted sender hosts)\
X-Ymailisg: CztoDCkWLDtUi6yd2Gm9ouRMdshq_VUfiaoHy7HLpiRW1RP0 RN6awkSG9aF6FGx8LTI2uQ3hJNMuDyZzN.sSZIMI5vEi9X7zpp6FyKmM6OGB 99Yude4ygXaXc0CSwTUtzO.V3KZe6C
X-Originating-Ip: [129.194.184.82]\
X-Originating-Ip: [192.168.1.100]\
Authentication-Results: mta1113.mail.ir2.yahoo.com  from=gelit.ch; domainkeys=neutral (no sig);  from=gelit.ch; dkim=neutral (no sig)\
Received: from 46.228.37.143 (46.228.37.143) by 188.125.84.238(188.125.84.238); Fri, 30 May 2014 14:16:46 +0000\
Received: from 127.0.0.1  (EHLO mail.gelit.ch) (129.194.184.82) by mta1113.mail.ir2.yahoo.com with SMTPS; Fri, 30 May 2014 14:16:45 +0000\
Received: from mbx01.interne.gelit.ch (192.168.1.13) by mbx01.interne.gelit.ch (192.168.1.13) with Microsoft SMTP Server (TLS) id 15.0.847.32; Fri, 30 M
Received: from mbx01.interne.gelit.ch ([fe80::6434:6464:437d:1a30]) by mbx01.interne.gelit.ch ([fe80::6434:6464:437d:1a30%12]) with mapi id 15.00.0847.0
Thread-Topic: test envoi\
Thread-Index: Ac98EZZlqOtAD9bmTnO6sRD8nYaNJw==\
Message-Id: <37fab99268444f7e8cc8a63cbe5c4ada@mbx01.interne.gelit.ch>\
Accept-Language: en-US, fr-CH\
Content-Language: en-US\
X-Ms-Has-Attach: \
X-Ms-Tnef-Correlator: \
Content-Type: multipart/alternative; boundary="_000_37fab99268444f7e8cc8a63cbe5c4adambx01internegelitch_"\
Mime-Version: 1.0\
Content-Length: 2094\
test envoi
```

Figure 8: Contenu du header du mail

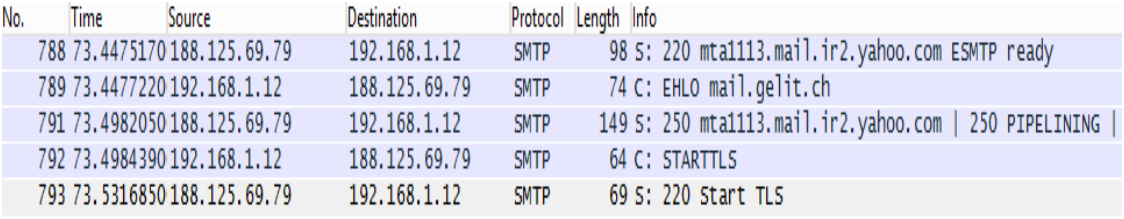
Dans les encadrés en vert, on a les différents éléments importants contenus dans le header :

- L'adresse mail de destination
- L'adresse mail de source
- IP externe de la source
- IP interne de la source

Tableau de routage du mail :

Hop	Delay	From	To	With	Time (UTC)
1	*	mbx01.interne.gelit.ch	mbx01.interne.gelit.ch	mapi	5/30/2014 2:16:20 PM
2	0 seconds	mbx01.interne.gelit.ch 192.168.1.13	mbx01.interne.gelit.ch 192.168.1.13	Microsoft SMTP Server (TLS)	5/30/2014 2:16:20 PM
3	25 seconds	EHLO 127.0.0.1	mta1113.mail.ir2.yahoo.com	SMTPS	5/30/2014 2:16:45 PM
4	1 Second	46.228.37.143	188.125.84.238		5/30/2014 2:16:46 PM

Figure 9: Tableau de routage du mail



No.	Time	Source	Destination	Protocol	Length	Info
788	73.4475170	188.125.69.79	192.168.1.12	SMTP	98	S: 220 mta1113.mail.ir2.yahoo.com ESMTP ready
789	73.4477220	192.168.1.12	188.125.69.79	SMTP	74	C: EHLO mail.gelit.ch
791	73.4982050	188.125.69.79	192.168.1.12	SMTP	149	S: 250 mta1113.mail.ir2.yahoo.com | 250 PIPELINING |
792	73.4984390	192.168.1.12	188.125.69.79	SMTP	64	C: STARTTLS
793	73.5316850	188.125.69.79	192.168.1.12	SMTP	69	S: 220 Start TLS

Figure 10: Capture Wireshark SMTP

Cette capture Wireshark illustre l'échange SMTP avec utilisation de TLS.

VI/ Scénario 2.c (signature)

6.1) Cahier des charges

Similaire au 2.1) avec les suppléments suivants

- Une autorité de certification (CA01.interne.gelit.ch)
- Qui peut délivrer les certificats et comment
- Délivrance de certificats clients pour signature des mails
- Interface web pour la requête
- Envoi et réception de mails signés
- Nombre de certificats :
    - Postes clients, 2 certificats : 1 personnel pour la signature + celui de la CA à mettre dans le *« trusted root certificate store »*
    - Serveurs Exchange, 2 certificats : 1 personnel pour les connexions SSL + celui de la CA à mettre dans le *« trusted root certificate store »*
- Ces certificats permettrons :
    - d'assurer le contrôle d'intégrité des mails échangés
    - la non-répudiation
    - la connexion SSL entre clients – CAS / CAS - MBX

6.2) Proposition de mise en œuvre de la PKI

Il est important de définir comment les certificats et les clefs privées seront délivrés. En effet, il est fondamental d'authentifier au préalable la personne qui les recevra. Elle devra pour cela se déplacer dans la structure responsable de la délivrance, afin d'effectuer la demande et de recevoir la clef privée et le certificat sur une clef USB.

6.2.1) Responsables

Il faut avoir une séparation des rôles dans la société. A cet effet, 2 utilisateurs ont été prévus afin d'avoir un *« two step verification process »* :

- CertRequester : le responsable fait une demande de certificat pour le client et vérifie les informations (il entre les différentes données du client (nom, prénom, adresse email), procède à l'identification physique…)
- CertManager : ce responsable délivre ou non le certificat après une deuxième vérification des informations

Permissions (au niveau du certificat mail signing) et rôle du CertRequester :

- Utilisateur du domaine
- Permissions Read & Enroll pour « Mail Signing » pour CertRequester
- Permission Read pour « Mail Signing » pour les « Authenticated user »
- Est le seul à pouvoir faire une demande de certificat *« Mail Signing »*
- Vérifie les informations du client
- Transmet la requête au CertManager
- Transmet la combinaison clef privée / certificat à l'utilisateur

Annexe 11.3)

Permissions (au niveau de la CA) et rôle du CertManager :

- Utilisateur du domaine
- Permissions *« Issue and Manage Certificates »* de la CA uniquement
- Se connecter à la CA par RDP
- N'a accès qu'aux demandes de certificats
- Vérifie les informations du client
- Approuve ou non la demande

Annexe 11.4)

Il faut mettre en place une GPO laissant à l'utilisateur l'accès à une seule console MMC, (pas mis en place dans ce projet)

Console du CertRequester :
La console MMC est spécifique et ne donne accès qu'au store où sont stockés les certificats dont la demande est acceptée (le store personnel) et qui peuvent être exportés.

Console du CertManager
A l'ouverture de la console MMC, l'utilisateur n'a accès qu'à la partie « pending » des requêtes de certificats de la CA. A partir de là, il peut vérifier les informations contenues dans la demande qu'il peut autoriser ou refuser.

6.2.2) Exemple de procédure simplifiée

1. Le client remplit un formulaire avec les données nécessaires et le donne au CertRequester (nom, prénom, email)
2. Le CertRequester ouvre un navigateur et rentre sur : https://192.168.1.11/certsrv. Il utilise ses données d'authentification : username : CertRequester, Password : HEpia10.
3. Il vérifie l'identité du demandeur puis entre les informations sur la page web.
4. Il soumet la requête à la CA
5. Le CertManager lance une connexion à la CA par le biais de RDP, puis utilise la console MMC spécifique (snap-in certification authority), vérifie les informations et l'identité une deuxième fois, puis accepte la requête
6. Le CertRequester retourne sur la page web et peut télécharger le certificat qui s'installera dans le magasin personnel de certificats.
7. Il exporte le certificat, le certificat de la CA, la clef privée et copie le tout sur une clef USB pour l'utilisateur
8. Suppression du certificat stocké dans le magasin personnel du CertRequester.

VII/ Test demande de certificats

7.1) Demande de certificats par IIS

- L'utilisateur CertRequester ouvre https://192.168.1.11/certsrv
- Il entre les données d'authentification (CertRequester / HEpia10)
- Puis il entre les données du client

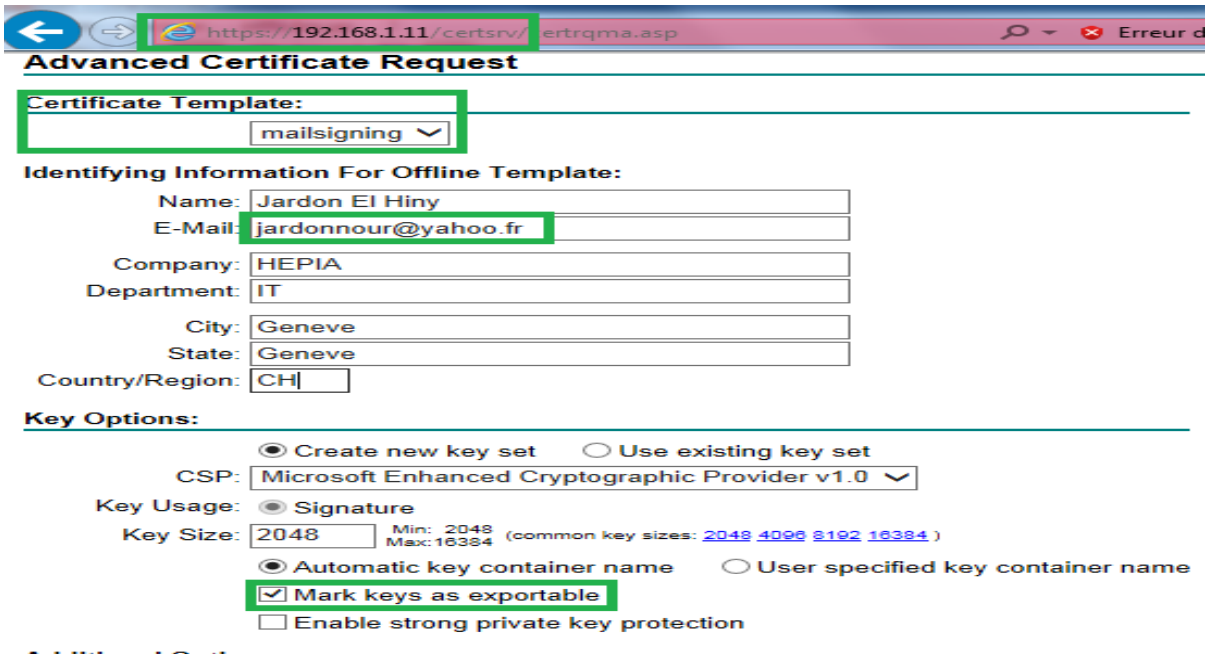


Figure 11: Interface WEB pour la requête de certificat

Une fois cette requête terminée, le CertManager ouvre une connexion RDP avec son login, sur la CA.

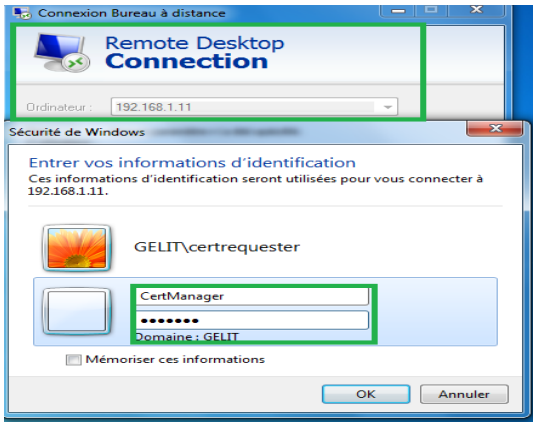


Figure 12: Connexion RDP du CertManager

L'utilisateur à accès à la console MMC, uniquement à l'onglet *« Pending Requests »*. Il peut donc vérifier les informations et délivrer le certificat.

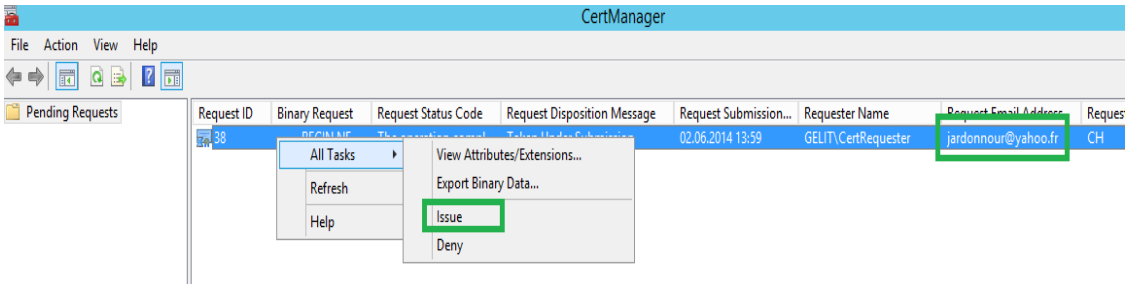


Figure 13: Acceptation de la demande par le CertManager

Le CertRequester retourne sur le site et va sur : *« view the status of a pending certificat request »* puis télécharge le certificat qui s'installe dans le magasin personnel. A partir de ce moment,, il peut exporter le certificat et la clef privée, stocker le tout sur la clef USB et la donner au client.
Voici le contenu du certificat une fois délivré

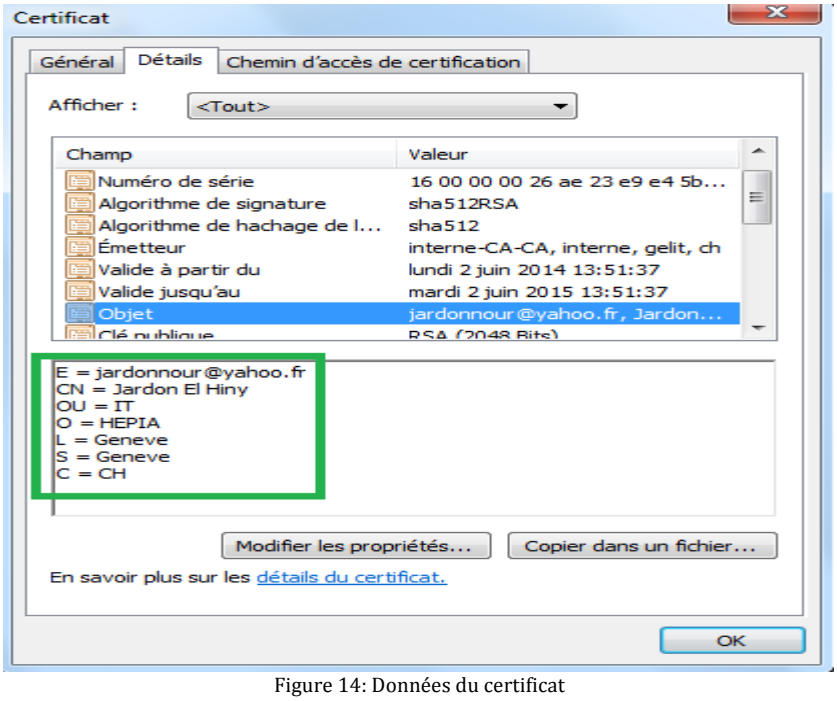


Figure 14: Données du certificat

VIII/ Scénario 2.d (chiffrement)

Ce scénario concerne exclusivement la problématique de la transmission des clefs publiques aux utilisateurs. La procédure est exactement la même que précédemment pour la signature, mais avec le modèle de certificat pour le chiffrement.

8.1) Cahier des charges

Similaire au 6.1 avec les suppléments suivants :

- Mise en place d'un modèle de certificat pour le chiffrement (mailcypher)
- Nombre de certificats :
    - Postes clients, 2 certificats principaux : 1 personnel pour le chiffrement + celui de la CA à mettre dans le *« trusted root certificate store »*
    - Autant de certificats (clefs publiques) que de contacts avec qui on communique

8.2) Configuration du certificat *« mailcypher »*

Veuillez suivre la procédure du 4.2.2, Scénario 1.
Certains éléments diffèrent. Comme les utilisateurs extérieurs ne sont pas membres du domaine, le certificat doit également avoir une fonction de signature (non-répudiation inutile). Ceci sert de Digital ID pour Outlook.
Cela lui permet d'utiliser le certificat (la clef publique) du destinataire pour ensuite chiffrer les mails. (Annexe 11.5)

8.3) Délivrance des certificats

Le plus difficile dans cette situation est d'obtenir la clef publique du correspondant afin de pouvoir chiffrer les mails. En effet, comme les utilisateurs ne sont pas tous membres du domaine, les clefs publiques doivent être transmises manuellement.

Plusieurs possibilités s'offrent :

- Le correspondant envoie la clef publique par email
- L'administrateur met sur un partage (SMB, FTP) ou une autre plateforme de partage les certificats qui seront accessibles par les contacts

Je m'intéresse à la deuxième possibilité.

Sur la CA, il n'est pas possible d'exporter les certificats qui ont été délivrés Il faut donc passer par un script Power Shell exécuté sur la CA (disponible en Annexe 11.6) qui permet d'exporter tous les certificats délivrés par la CA et de les stocker dans un dossier. L'administrateur peut ensuite les prendre et les mettre à la disposition des clients.

IX/ Test du script Power Shell

A l'exécution du script, tous les certificats qui ont été délivrés et qui se trouvent dans le dossier *« Issued Certificates »* sont bien exportés dans le dossier test.

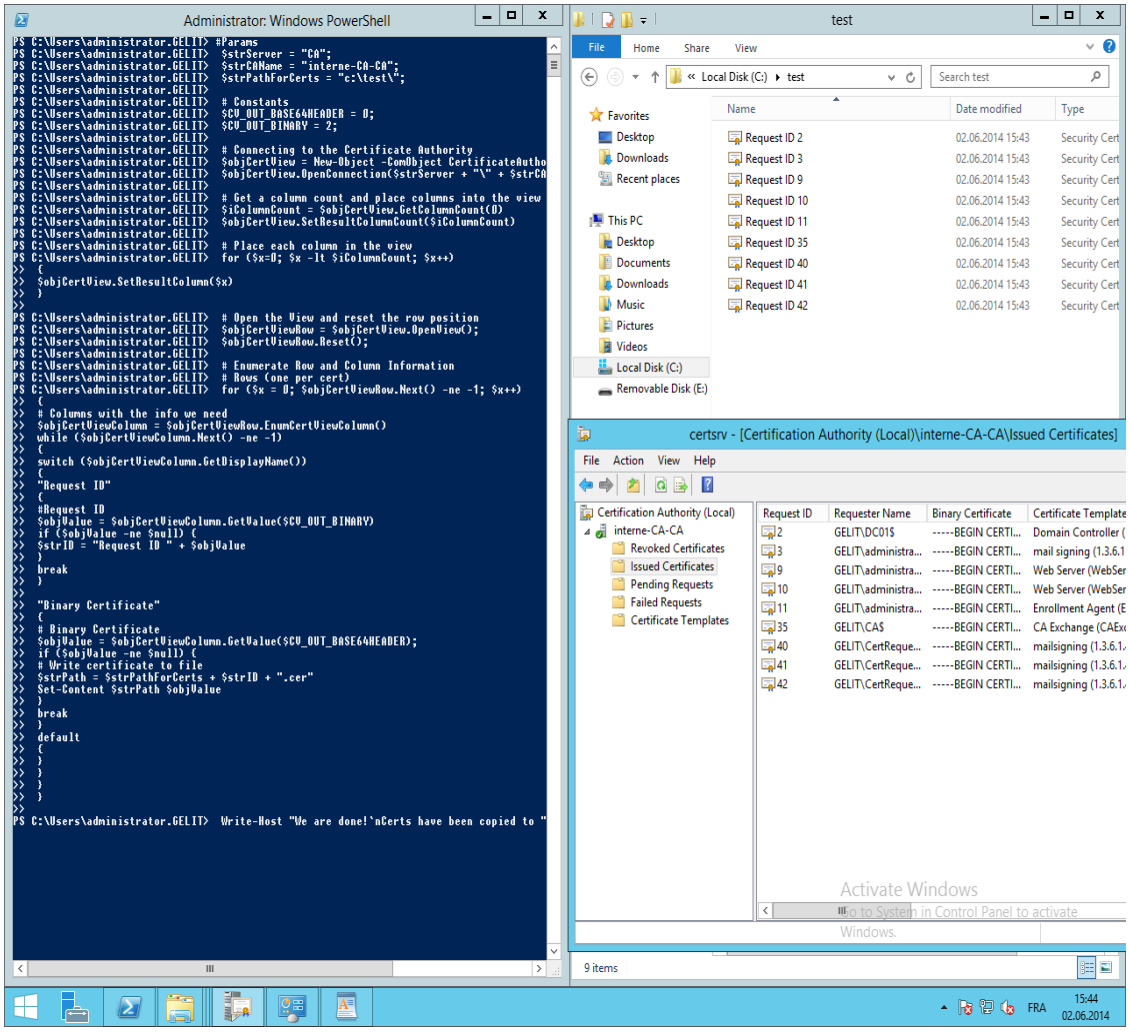


Figure 15: Résultat du script Power Shell

X/ Conclusion

Cette deuxième partie a permis de poursuivre la mise en place du système de messagerie, cette fois-ci, pour l'échange de mails avec l'extérieur. J'ai été confronté à des problèmes de sécurité en ce qui concerne le DNS et les connecteurs Exchange. Il faut bien avoir une séparation entre le serveur DNS et le serveur DNS externe afin de ne pas dévoiler la configuration du réseau à l'extérieur. Il a fallu également faire attention aux ports à utiliser (HTTPS et SMTP uniquement) et à l'emplacement physique du CAS (sur le réseau interne uniquement). Cette partie m'a permis également de comprendre la fonction des différents connecteurs d'Exchange pour la transmission des mails. En effet, par défaut, il n'y a aucune sécurité et ils offrent un maximum de connectivité. Il est donc nécessaire de modifier les paramètres en fonction des besoins pour limiter les risques. Les analyses Wireshark m'ont également permis de comprendre comment se fait l'échange des mails, la négociation de la sécurité, les protocoles et ports utilisés. En effet, Exchange peut, avec un autre serveur SMTP compatible ESMTP, initier des connexions TLS, si cela est spécifié dans le connecteur. C'est donc dans ce cas, une négociation automatique avec le partenaire, soit une connexion TLS soit une connexion non chiffrée.

Il m'a été également possible de configurer et d'utiliser mon Smartphone pour l'échange de mails, signés et chiffrés sans aucun problème afin de pousser les tests plus loin et de m'assurer de la compatibilité.

XI/ Annexes

11.1) Connecteurs de réception

Configuration pour le CAS01 (Default Front End)

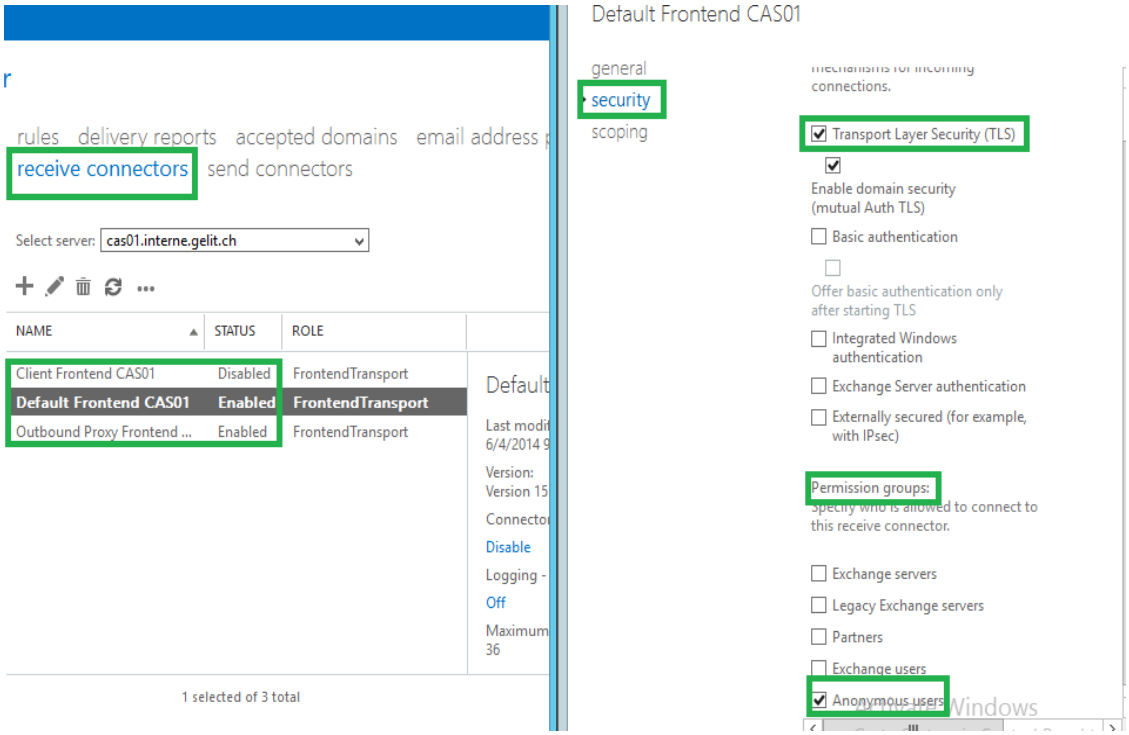


Figure 16: Sécurité du connecteur Default Frontend

Configuration pour le CAS01 (Outbound Proxy)

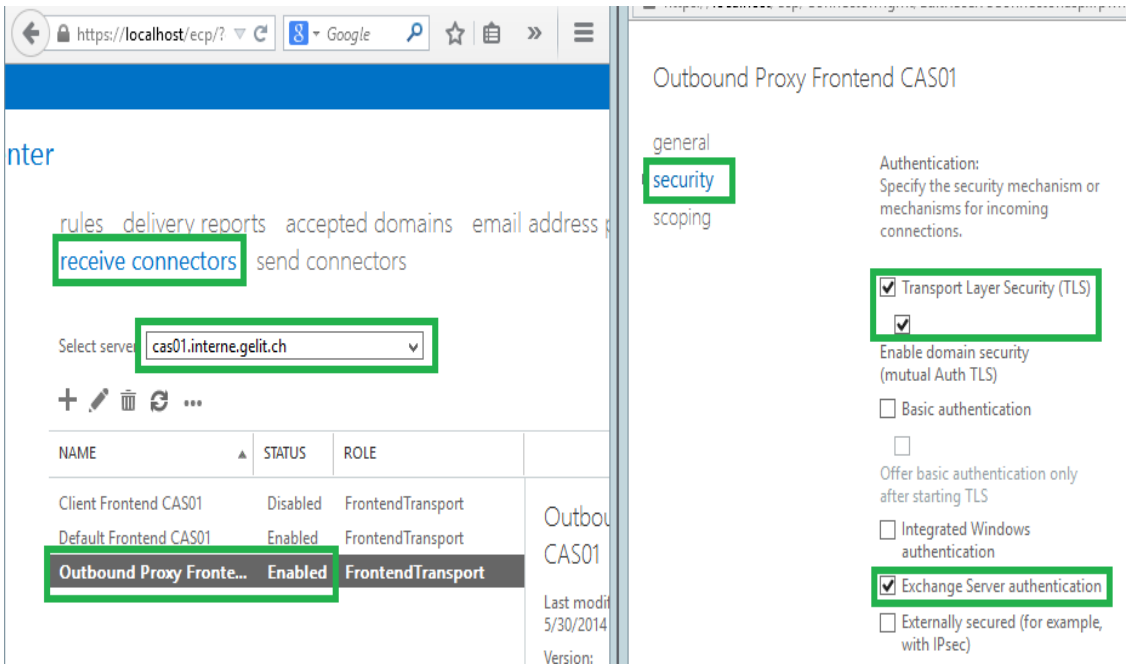


Figure 17: Sécurité du connecteur Outbound Proxy Frontend

Configuration pour le MBX01 (receiver)

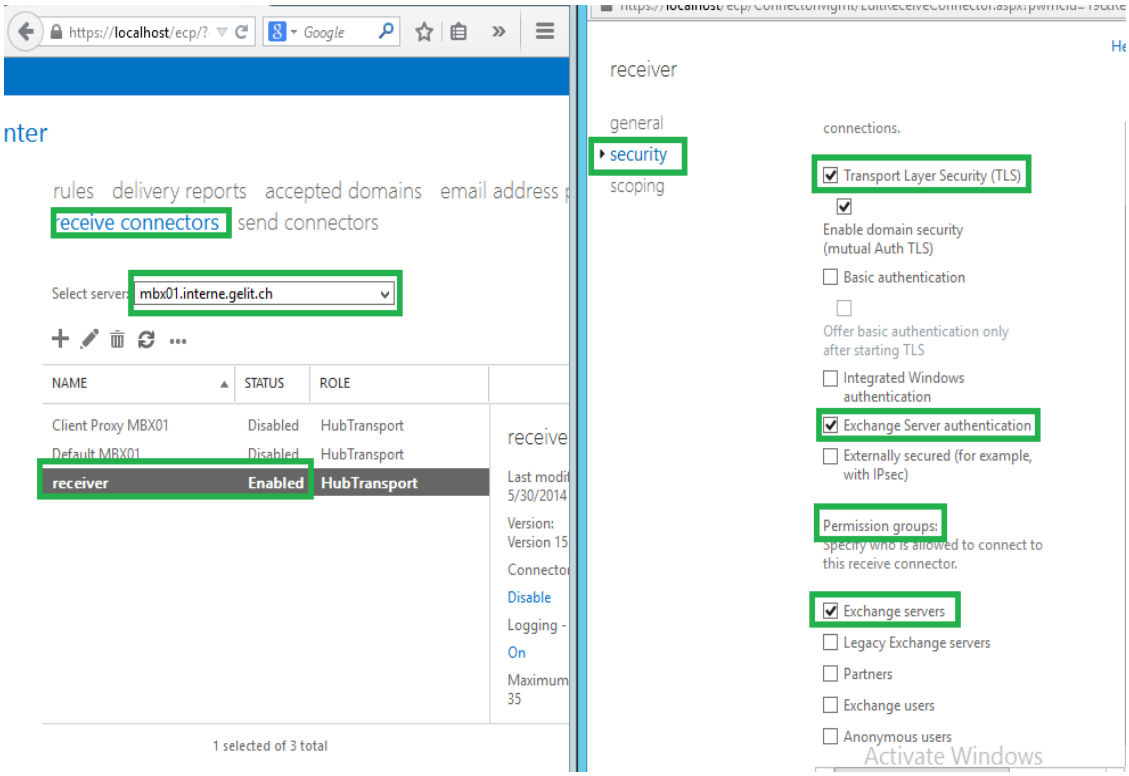


Figure 18: Sécurité du connecteur Receiver

11.2) Connecteurs d'envoi

Configuration du MBX01

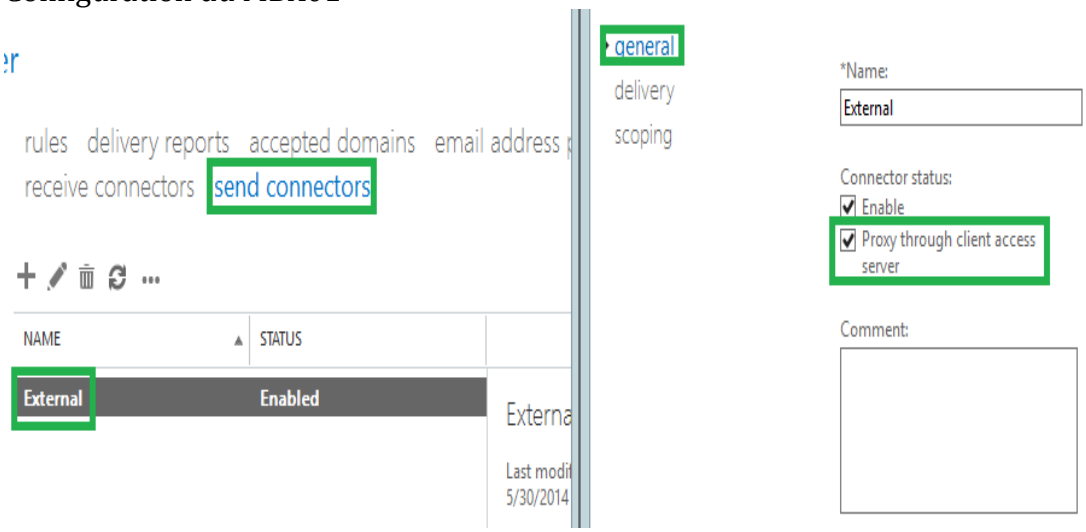


Figure 19: Connecteur d'envoi

11.3) Permissions du CertRequester

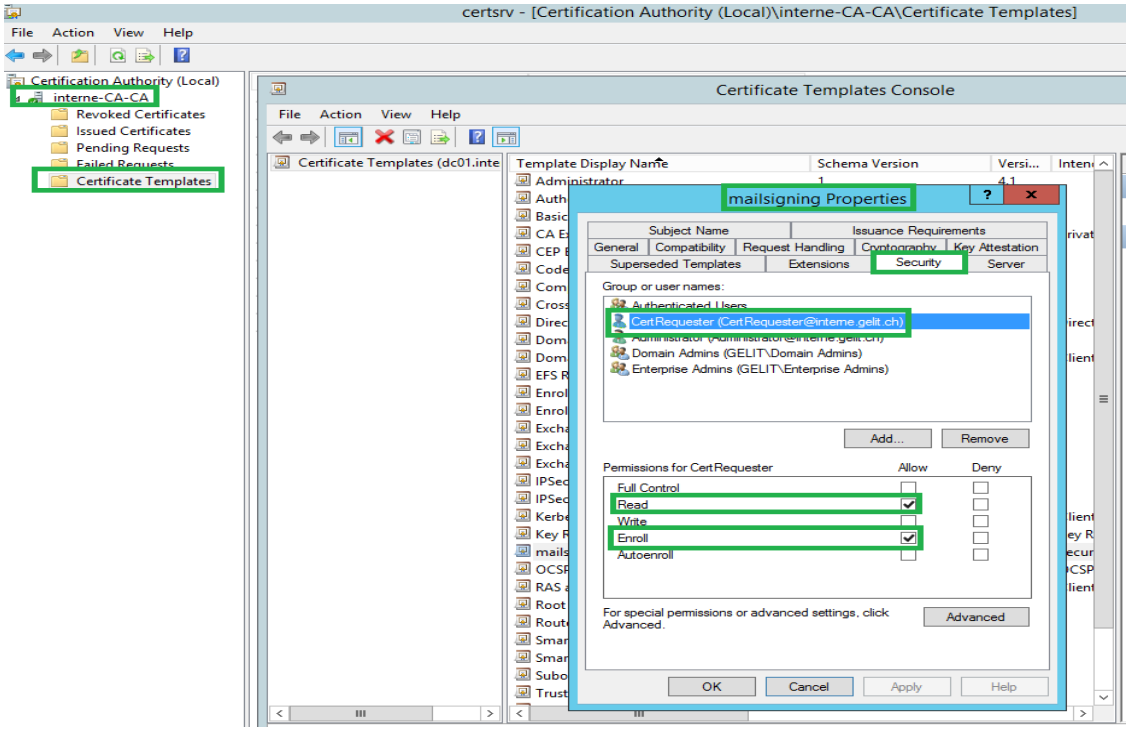


Figure 20: Permissions du CertRequester

11.4) Permissions du CertManager

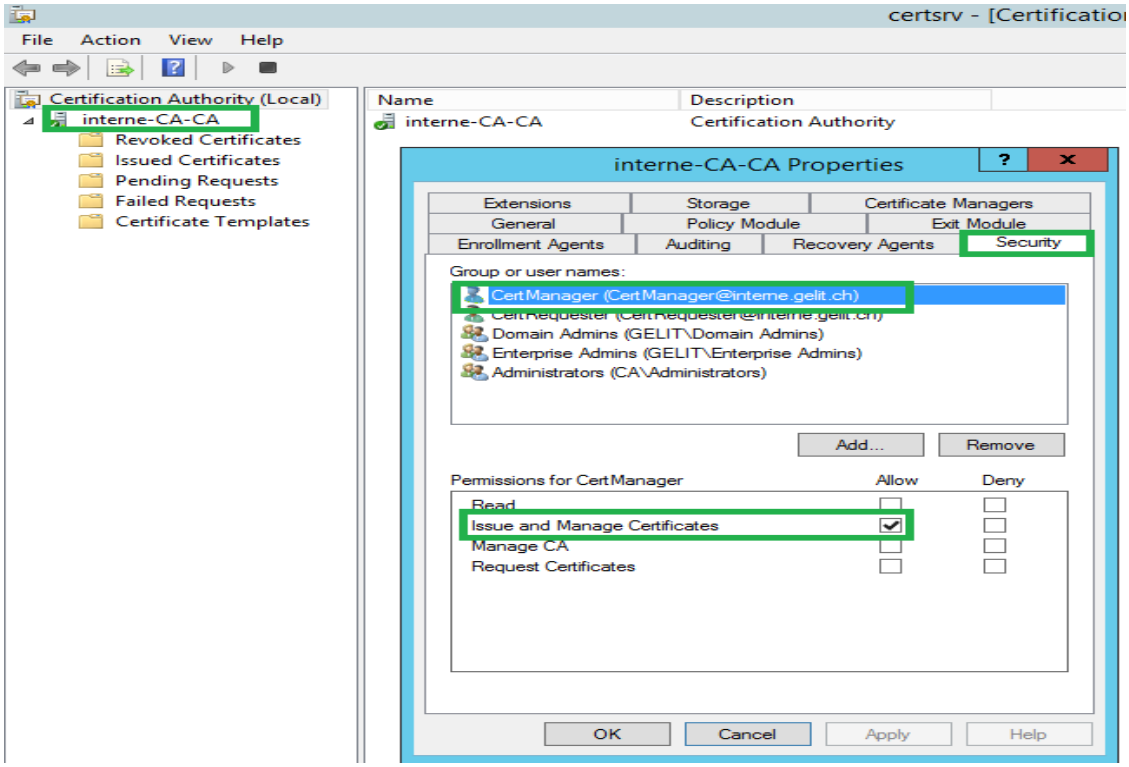


Figure 21: Permissions du CertManager

11.5) Certificat « mailcypher »

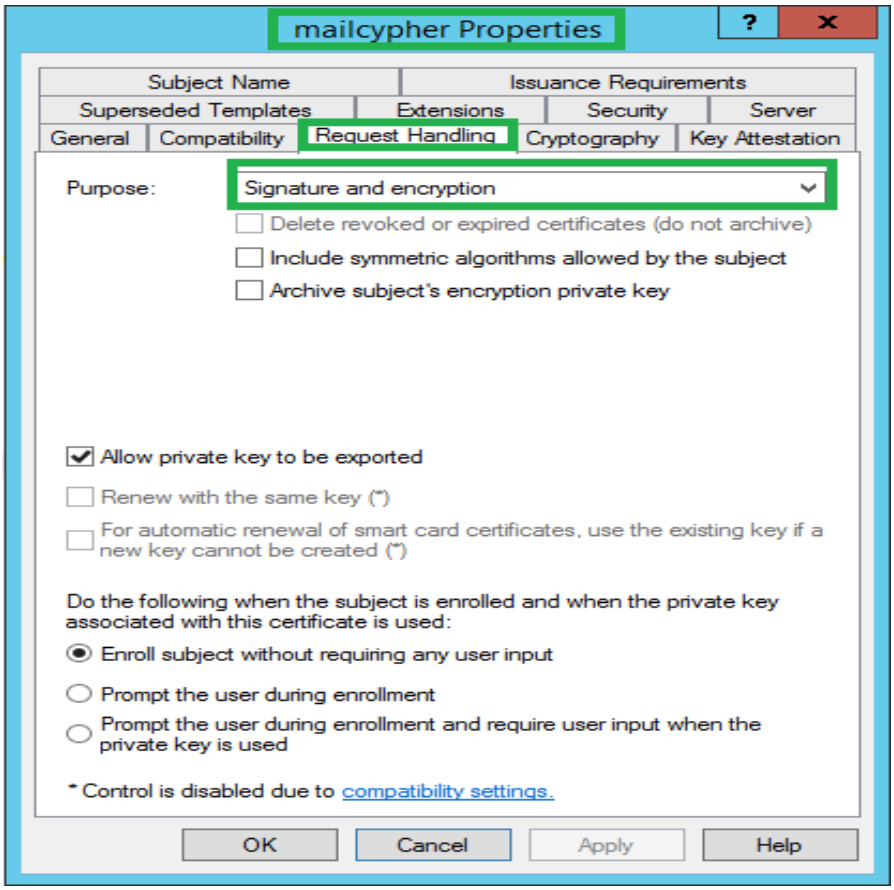


Figure 22: But du certificat « mailcypher »

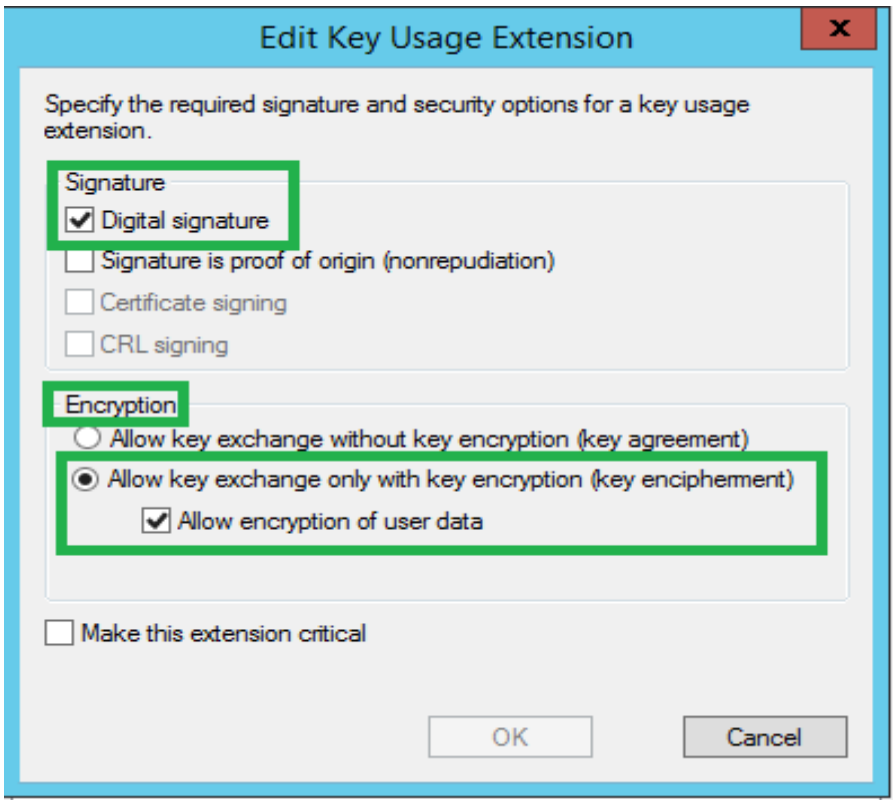


Figure 23: Utilisation des clefs

11.6) Script Power Shell[9]

```
#Params
 $strServer = "ca01";
 $strCAName = "mydomain-CA01-CA";
 $strPathForCerts = "c:\test\";

 # Constants
 $CV_OUT_BASE64HEADER = 0;
 $CV_OUT_BINARY = 2;

 # Connecting to the Certificate Authority
 $objCertView = New-Object -ComObject CertificateAuthority.View
 $objCertView.OpenConnection($strServer + "\" + $strCAName)

 # Get a column count and place columns into the view
 $iColumnCount = $objCertView.GetColumnCount(0)
 $objCertView.SetResultColumnCount($iColumnCount)

 # Place each column in the view
 for ($x=0; $x -lt $iColumnCount; $x++)
 {
 $objCertView.SetResultColumn($x)
 }

 # Open the View and reset the row position
 $objCertViewRow = $objCertView.OpenView();
 $objCertViewRow.Reset();

 # Enumerate Row and Column Information
 # Rows (one per cert)
 for ($x = 0; $objCertViewRow.Next() -ne -1; $x++)
 {
 # Columns with the info we need
 $objCertViewColumn = $objCertViewRow.EnumCertViewColumn()
 while ($objCertViewColumn.Next() -ne -1)
 {
 switch ($objCertViewColumn.GetDisplayName())
 {
 "Request ID"
 {
 #Request ID
 $objValue = $objCertViewColumn.GetValue($CV_OUT_BINARY)
 if ($objValue -ne $null) {
 $strID = "Request ID " + $objValue
 }
 break
 }

 "Binary Certificate"
 {
 # Binary Certificate
 $objValue = $objCertViewColumn.GetValue($CV_OUT_BASE64HEADER);
 if ($objValue -ne $null) {
 # Write certificate to file
 $strPath = $strPathForCerts + $strID + ".cer"
 Set-Content $strPath $objValue
 } break
 }default
 {}} } }
 Write-Host "We are done!`nCerts have been copied to " + $strPathForCerts
```

[9] http://blogs.msdn.com/b/alejacma/archive/2012/04/13/how-to-export-issued-certificates-from-a-ca-programatically-powershell.aspx

Scénario 3

Haute disponibilité Exchange
Internet

I/ Introduction

1.1) Contexte

L'étude de cette partie du projet porte sur la haute disponibilité de l'infrastructure de messagerie basée sur les produits Microsoft (Windows Server 2012 & Exchange 2013) avec la transmission de mails sur Internet. Ce travail se fera en salle de laboratoire de l'HEPIA afin de pouvoir effectuer les différentes installations des logiciels et systèmes d'exploitation, configurations et tests avant une éventuelle mise en production.
Plusieurs configurations sont possibles et je passerai en revue les différentes possibilités. La mise en œuvre d'un système de NLB pour la haute disponibilité des CASs et d'un cluster DAG (Database Availability Group) pour la haute disponibilité des MBXs sera effectuée afin d'assurer la redondance.

1.2) Schéma

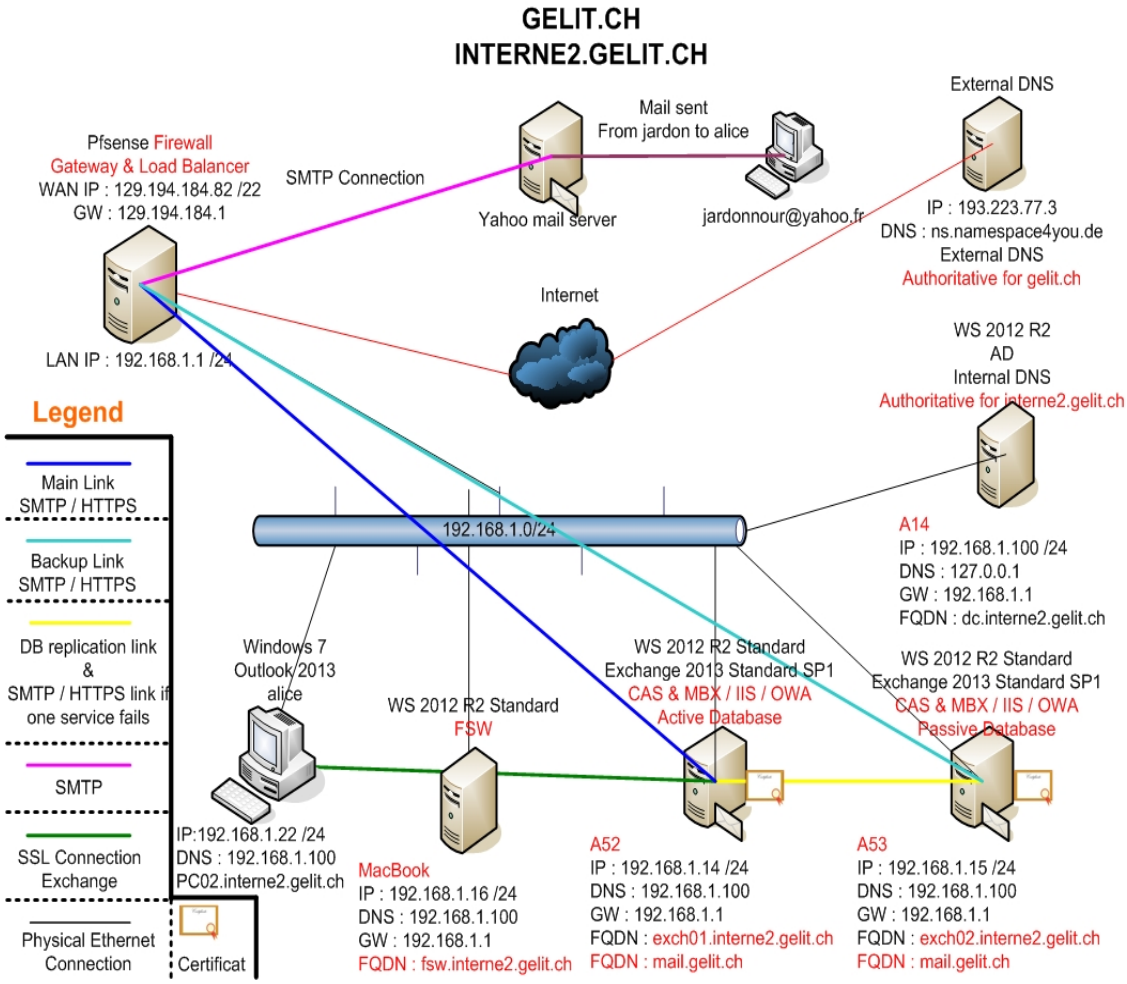


Figure 1 : Schéma de l'installation

1.3) Topologie physique

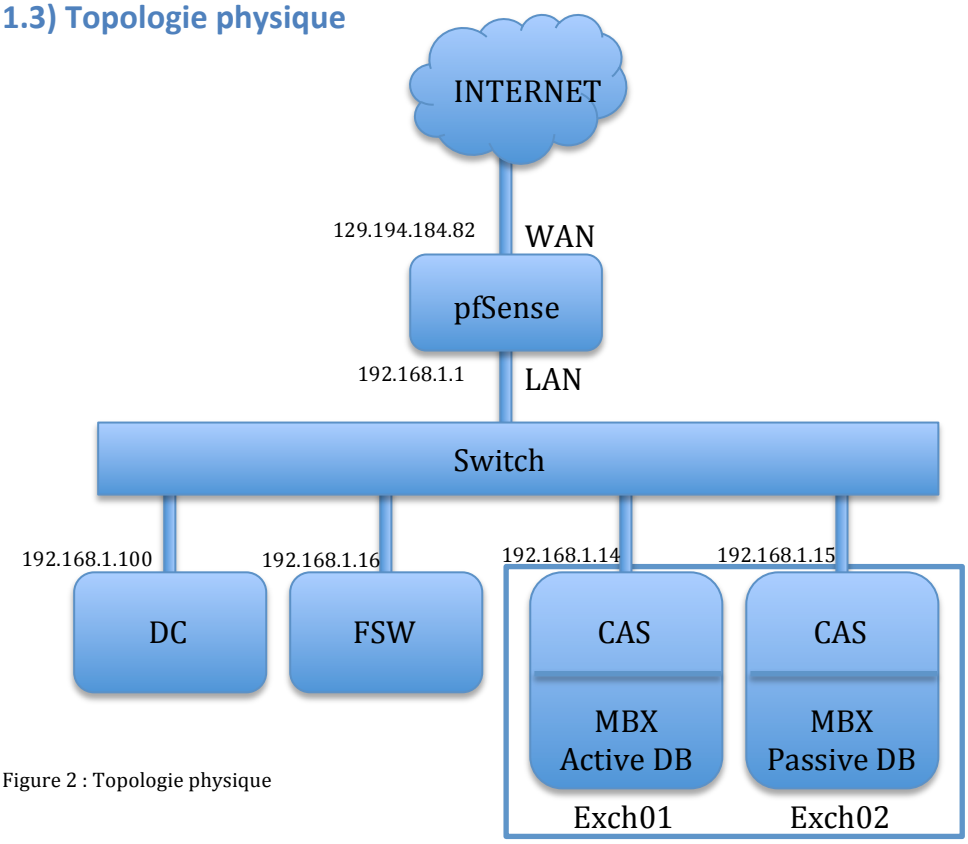


Figure 2 : Topologie physique

1.4) Analyse

Avec Exchange 2013, la mise en place de la haute disponibilité a quelque peu changé depuis la modification des rôles. La haute disponibilité permet de faire face à des problèmes de pannes (logiciels ou matériels) ou de surcharges des serveurs et de procéder à des opérations de maintenance sur les serveurs, tout en assurant la continuité des services offerts. Comment implanter cette haute disponibilité ? Différentes variantes sont possibles en fonction d'une architecture serveur mono-rôle ou multi-rôles. La gestion de la haute disponibilité est différente en fonction des rôles. La HD du CAS est assurée par un système de répartition de charge ou de failover. C'est ce dernier système qui sera adopté pour le MBX par la mise en place d'un cluster (DAG).

Un autre élément important est la gestion des certificats des CAS. Afin d'éviter toute coupure de connexion pour le client, les CASs doivent posséder le même certificat SAN. Un DAG peut être composé des versions standard et entreprise d'Exchange qui doivent toutefois posséder strictement le même système d'exploitation.

Prérequis supplémentaire : *http://technet.microsoft.com/en-us/library/dd638104(v=exchg.150).aspx*

Dans cette partie, j'aborde les notions suivantes :

- Changements importants avec Exchange 2013 et les versions précédentes
- Comparaison de la haute disponibilité mono-rôle et multi-rôles
- Connecteurs Exchange
- Failover
- File Share Witness (FSW) et Cluster
- Bases de données et réplication
- DNS Round Robin et Backup MX

La gestion des connecteurs est également à revoir. Dans une infrastructure multi-rôles, les connecteurs sont quelque peu différents.

1.4.1) Changements avec Exchange 2013

Changements importants :

- HLB de niveau 4 au lieu de 7 pour le CAS : détecte l'indisponibilité des services (SMTP, HTTPS)
    - Economie, coût moindre du matériel, efficace
- Pas d'affinité de session
    - Load balancing ou failover transparent
- Cookie d'authentification chiffré par le certificat du CAS après le login pour permettre une connexion à un autre CAS sans avoir besoin de se ré-authentifier
    - Nécessité de posséder le même certificat pour les 2 CAS
- DNS Round Robin pas recommandé
    - N'est pas considéré comme un système de haute disponibilité
    - Ne détecte pas les pannes et ne redirige pas les connexions de manière intelligente
    - Risque de pertes de connexions en cas de perte d'un CAS
    - En cas de panne d'un serveur Exchange, pour deux entrées DNS, 50% des connexions sont perdues
- Jusqu'à 100 bases de données par serveur dans un DAG (16 serveurs maximum)
- Le DAG fait appel au service cluster de Windows Server 2012
- Shadow Redundancy : protège les messages en transit. Suppression du message de la base de données de transport que si le message est bien arrivé au *« next hop »*
- Nécessité d'un File Share Witness (FSW) pour le DAG (serveur séparé))
- Système de votation pour la gestion du cluster

1.4.2) Variantes de haute disponibilité

Dans le cadre d'un déploiement avec serveurs multi-rôles (variante 1)

Avantages :

- Meilleure utilisation des ressources du serveur
- Meilleur rendement des serveurs pour les petites sociétés
- Coûts moindres
- Administration et configuration simplifiées
- 2 serveurs Exchange suffisent

Inconvénients :

- Problèmes de sécurité : le MBX est exposé sur Internet
- Question quant à la véritable utilité du CAS en tant que proxy
- Plantage du système = perte de la configuration et des bases de données en même temps (long délai de remise en service)
- Problèmes de performance en cas d'utilisation intensive des serveurs
- Windows Network Load Balancing (WNLB) pour le CAS
    - Incompatible avec le cluster DAG des MBX
    - Impacte négativement sur le réseau (port flooding)
    - Détection au niveau serveur (IP) et non de services

- HLB ou NLB nécessaire pour la haute disponibilité du CAS (coût élevé)
- Limitations techniques avec la virtualisation (limitation vCPU…)
-

Dans le cadre d'un déploiement avec serveurs à rôles séparés (variante 2)

Avantages :

- Plus grande flexibilité (ajouts, suppressions de serveurs et de rôles)
- Meilleures performances en cas de forte utilisation
- Sécurité accrue : seul le CAS est exposé sur Internet
- Si un serveur plante, un seul rôle plante
- WNLB possible, mais toujours pas recommandé
- SLB ou HLB recommandé

Inconvénients :

- Prix élevé du matériel, des logiciels et des licences
- Coûts de la maintenance
- Administration plus complexe, plus de serveurs à configurer, à gérer et à sécuriser
- Disparité des configurations et du matériel des serveurs (gestion et maintenance plus difficiles)
- Au minimum 4 serveurs Exchange pour assurer une très haute disponibilité

Dans le cadre de ce projet, seule la variante 1 est envisagée.

Variante 1, schéma simplifié de haute disponibilité

Une seule DB Exchange principale
Une copie active sur Exch01
Une copie passive sur Exch02
Haute disponibilité de type failover

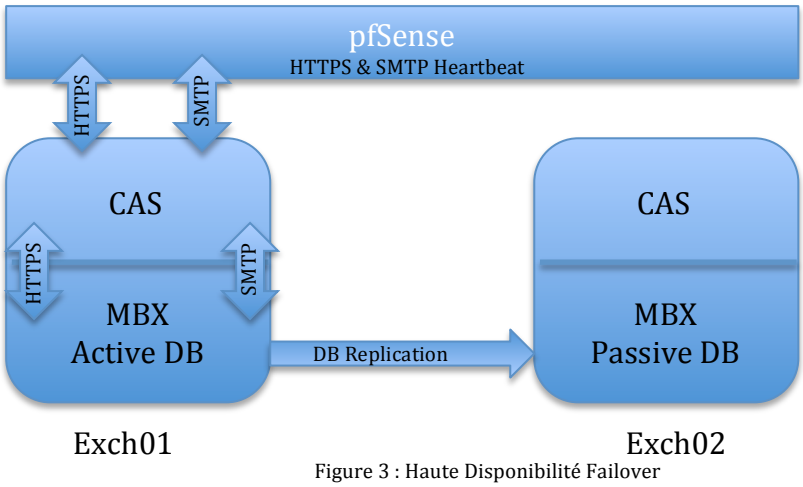


Figure 3 : Haute Disponibilité Failover

Lorsqu'un client ou un serveur externe initie une connexion, pfSense redirige la connexion sur le CAS de Exch01. Il y a 2 bases de données, une active sur Exch01 et une passive sur Exch02. Les mails sont stockés sur Exch01 puis répliqués sur Exch02 par le service de réplication d'Exchange.

Que se passe-t-il en cas de panne complète de Exch01 ?

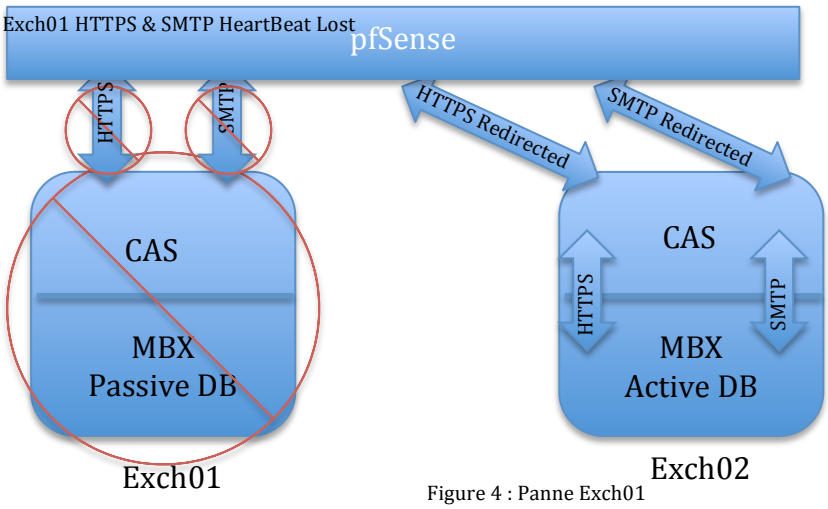


Figure 4 : Panne Exch01

Lorsque le serveur Exch01 tombe en panne, pfSense le diagnostique grâce à la perte des HeartBeats des services HTTPS et SMTP d'Exchange. Il redirige alors toutes les requêtes vers le rôle CAS de Exch02. Le cluster détermine que Exch01 est en panne et Exchange met la DB de Exch02 en actif. Le système de réplication reste indisponible jusqu'à ce que Exch01 revienne en ligne.

1.4.3) Connecteurs Exchange

Pour les informations de base, se référer au 1.3.1 du scénario 1.
Etant donné qu'on utilise une infrastructure serveur multi-rôles, les connecteurs sont quelque peu différents., Les connecteurs entre Exch01 et Exch02 sont les mêmes, mais il faut les modifier afin d'améliorer la sécurité et pour pouvoir gérer les flux SMTP. Je ne montre ici que les changements à effectuer pour Exch01.

Pour le connecteur d'émission, il faut simplement spécifier de passer par le proxy du CAS et que Exch01 et Exch02 sont les serveurs responsables de l'émission.

Pour les connecteurs de réception, sur les cinq serveurs qui sont créés par défaut, deux sont à désactiver et trois à modifier. Je ne liste ici que les trois à modifier :

1. Default FrontEnd Exch01 (pour le rôle CAS)
2. Outbound Proxy FrontEnd Exch01 (pour la fonction proxy)
3. Default Exch01 (pour le rôle MBX)

Au niveau des ports, il y a quelques changements :

- Le connecteur 1 utilise le port 25 pour la réception des mails du CAS
- Le connecteur 2 utilise le 717 en écoute pour le proxy CAS
- Le connecteur 3 est un connecteur SMTP du rôle MBX., mais étant donné que les connecteurs 1 et 3 ne peuvent pas utiliser le même port (car ils sont sur le même serveur), ce dernier utilise alors le port 2525

Connecteur 2 : la fonction proxy du rôle CAS doit pouvoir accepter les connexions du rôle MBX de Exch01 et Exch02 UNIQUEMENT pour l'envoi de mails.
Outbound SMTP :

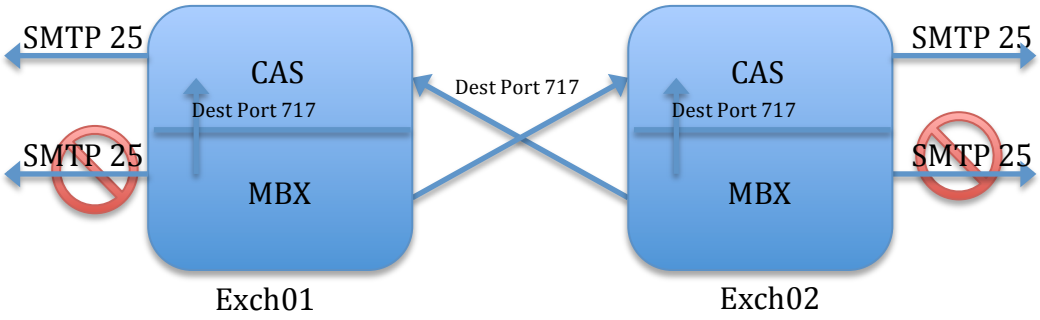


Figure 5 : Flux Outbound SMTP

Connecteur 3 : Le rôle MBX de Exch01 et Exch02 doit pouvoir accepter les connexions du rôle CAS de Exch01 et Exch02 UNIQUEMENT.
Inbound SMTP :

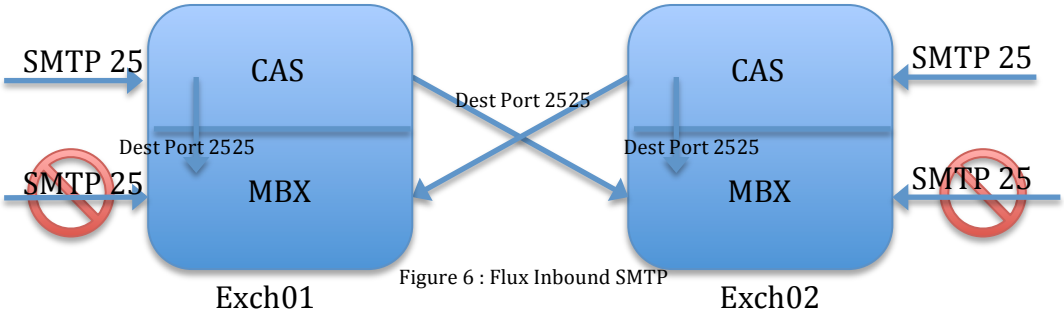


Figure 6 : Flux Inbound SMTP

1.4.4) Failover

Pour ce projet, j'utilise pfSense comme firewall, passerelle, mais également comme système de failover. Plusieurs possibilités s'offrent :

- Loadbalancing
- Automated Failover
- Manual Failover

Pour les services SMTP et HTTPS avec Exchange 2013, PfSense se montre efficace avec « l'automated failover ». C'est ce qui est utilisé ici. Exch01 est le serveur principal et toutes les connexions sont redirigées vers ce serveur. Rien ne passe par Exch02 tant que tout est fonctionnel avec Exch01. PfSense surveille les services HTTPS et SMTP grâce aux « monitors » et peut indépendamment rediriger les requêtes d'un serveur à l'autre en fonction du protocole.

Si Exch01 tombe en panne, pfSense redirige les requêtes (HTTPS & SMTP) vers Exch02.

Si un service HTTPS ou SMTP de Exch01 tombe en panne (imaginons que ce soit HTTPS), alors seules les requêtes HTTPS sont redirigées vers Exch02 et Exch01 continue de traiter les requêtes SMTP.

Exemple : Fonctionnement normal

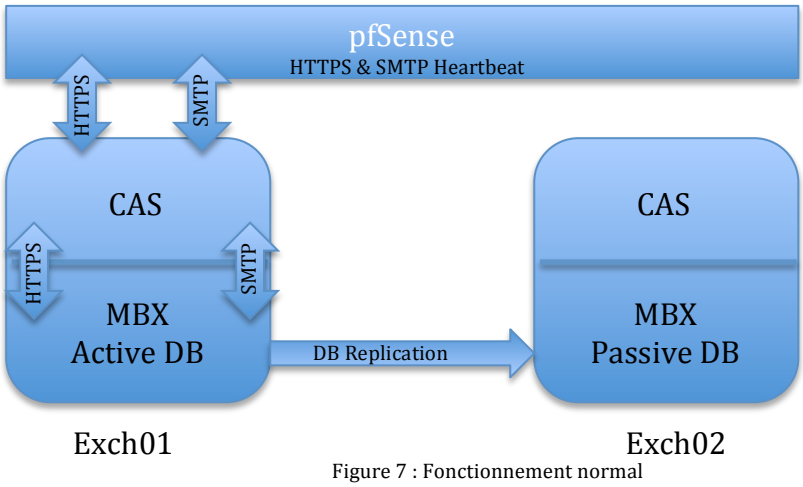


Figure 7 : Fonctionnement normal

Exemple : panne du service HTTPS du CAS de Exch01

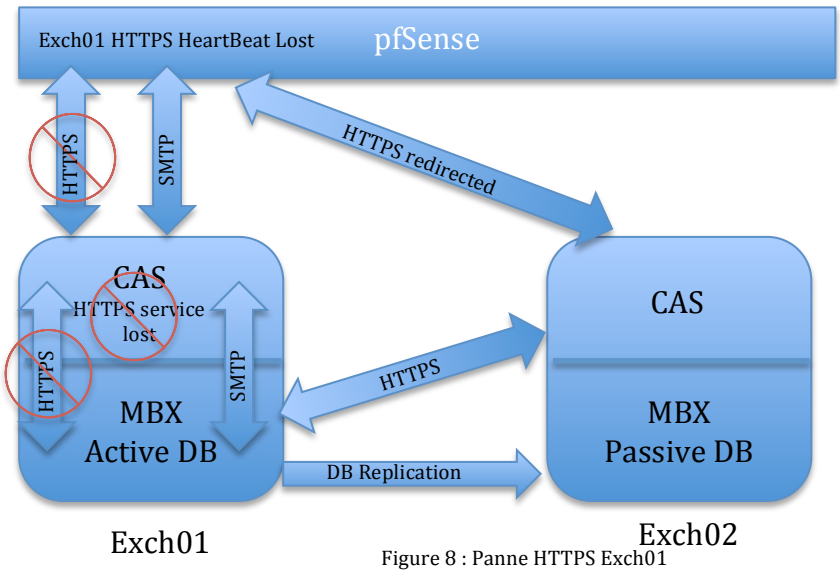


Figure 8 : Panne HTTPS Exch01

1.4.5) DAG, FSW, Cluster

Afin d'assurer la haute disponibilité de la base de données Exchange, on fait appel au DAG dont le fonctionnement repose sur la fonctionnalité du service cluster de Windows. L'installation et la configuration de ce service se font automatiquement par Exchange lors de la création du DAG.

Il est indispensable de maintenir en vie le cluster et pour cela il faut savoir dans quel cas le cluster peut tomber en panne et la BDD d'Exchange se « démonter », rendant la messagerie indisponible.

Le maintien du cluster, aussi appelé maintien du Quorum, se fait par le biais d'un système de votation où chaque serveur Exchange possède un droit de vote. Cette votation est essentielle. On pourrait penser qu'il est suffisant de disposer de deux serveurs Exchange pour maintenir le cluster et les services Exchange en vie. C'est

faux. Si l'on a un nombre pair de serveurs Exchange, il faut un FSW pour maintenir le cluster en vie et pour que la base de données soit disponible.
Dans la configuration actuelle avec deux serveurs Exchange :

- Sans FSW : si un des deux serveurs Exchange tombe,,en panne, le cluster et la DB sont en panne et les services Exchange sont indisponibles
- Avec FSW : si un des deux serveurs Exchange tombe en panne, le cluster et la BDD restent en vie et il n'y a pas d'indisponibilité

Le FSW fait appel au service de partage de fichiers et de partage d'un dossier. Le FSW ne doit pas être un contrôleur de domaine et il n'est pas conseillé de l'utiliser sur un serveur Exchange.

1.4.6) Bases de données et réplication

1.4.6.1) Bases de données

Pour assurer le bon fonctionnement du DAG ainsi que du processus de réplication, il y a quelques prérequis très importants :

6)"Up to 16 copies of an Exchange 2013 mailbox database can be created on multiple Mailbox servers, provided the servers are grouped into a database availability group (DAG), which is a boundary for continuous replication. Exchange 2013 mailbox databases can be replicated only to other Exchange 2013 Mailbox servers within a DAG. You can't replicate a database outside of a DAG, nor can you replicate an Exchange 2013 mailbox database to a server running Exchange 2010 or earlier. For detailed information about DAGs, see Database Availability Groups.
7)All Mailbox servers in a DAG must be in the same Active Directory domain.
8)Mailbox database copies support the concepts of replay lag time and truncation lag time. Appropriate planning must be performed before enabling these features.
9)All database copies can be backed up using an Exchange-aware, Volume Shadow Copy Service (VSS)-based backup application.
10) Database copies can be created only on Mailbox servers that don't host the active copy of a database. You can't create two copies of the same database on the same server.
11) All copies of a database use the same path on each server containing a copy. The database and log file paths for a database copy on each Mailbox server must not conflict with any other database paths.
12) Database copies can be created in the same or different Active Directory sites, and on the same or different network subnets.
Database copies aren't supported between Mailbox servers with round trip network latency greater than 500 milliseconds (ms)"[10]

[10] http://technet.microsoft.com/en-us/library/dd979802(v=exchg.150).aspx

1.4.6.2) Réplication

Il existe plusieurs types de réplications pour Exchange :

- Synchrone (nécessite un « third party replication API)
- Asynchrone (nécessite un « third party replication API)
- Continue (natif)

En mode de réplication synchrone, lorsque Exchange effectue une écriture sur le disque, il ne reçoit la confirmation que lorsque tous les systèmes de stockage en réplication ont écrit les données.

En mode de réplication asynchrone, Exchange reçoit une confirmation d'écriture dès qu'il a écrit sur le premier système de stockage. Exchange n'est pas au courant de la réplication entre les systèmes de stockage. On est en service « best effort ».

La réplication continue, quant à elle, est un processus logiciel spécifique intégré à Exchange lors de l'utilisation d'un DAG pour la haute disponibilité. Les détails de cette réplication sont fournis plus bas.

"Each DAG member hosting a copy of a given mailbox database participates in a process of continuous replication to keep the copies consistent. Database replication occurs between Exchange Server 2013 DAG members using two different methods:

***File Mode replication** – each transaction log is fully written (a 1MB log file) and then copied from the DAG member hosting the active database copy to each DAG member that host a passive database copy of that database.*
The other DAG members then replay the transaction log file into their own passive copy of the database to update it. File mode replication has an obvious downside in that a transaction log that hasn't already been copied to the other DAG members may be lost if the DAG member hosting the active database copy becomes unavailable. Although there are other recovery mechanisms to minimize the impact of this scenario, this is a reason why file mode replication is used only during the initial seeding of a database copy.
After seeding is complete the database switches automatically to block mode replication.

***Block mode replication** – as each database transaction is written to the log buffer on the active server and also sent to the log buffer of DAG members hosting passive copies of the database. As the log buffer becomes full members of the DAG are then able to build their own transaction log file for replay into their passive database copy. Block mode replication has advantages compared to file mode replication when there is a failure in the DAG, because less transaction log data is likely to be lost."*[11]

[11] http://exchangeserverpro.com/exchange-server-2013-database-availability-groups/

1.4.7) Certificats Exchange

Lorsque un système de load balancing ou de failover est utilisé, il est important de prendre un compte comment sont gérées les connexions des utilisateurs et les certificats d'Exchange. Avec Exchange 2013, lorsqu'un utilisateur se log, un cookie d'authentification est délivré puis chiffré par le certificat du CAS. Si l'utilisateur change de CAS par load balancing ou failover, et que les CAS ne possèdent pas les mêmes certificats, alors l'utilisateur devra se ré-authentifier car le déchiffrement du cookie ne sera pas possible. Si les certificats Exchange des CASs sont les mêmes, alors ce processus sera transparent pour l'utilisateur et il n'aura pas besoin de s'authentifier à nouveau. En effet, le deuxième CAS sera en mesure de déchiffrer le cookie.
http://theucguy.net/exchange-server-2013-load-balancing/

II/ Scénario

2.1) Cahier des charges

Dans ce projet de mise en place d'une messagerie de haute disponibilité, les différents services, logiciels et matériels ainsi que les divers prérequis sont les suivants:

- Un nom de domaine public = gelit.ch
- Un nom de sous-domaine interne basé sur le public : interne2.gelit.ch
- Zone DNS publique pour les requêtes externes = gelit.ch
- Zone DNS interne pour les requêtes internes : interne2.gelit.ch
- Un serveur Active directory (DC.interne2.gelit.ch)
- Un serveur FileShareWitness (FSW.interne2.gelit.ch)
- Enregistrement des records A des serveurs et postes clients
- Infrastructure Serveurs Multi-rôles
- Deux serveurs Exchange 2013 SP1
    - Exch01.interne2.gelit.ch
    - Exch02.interne2.gelit.ch
- pfSense (Firewall + HLB)
- Windows Server 2012 Standard pour tous les serveurs
- 2 postes clients membres du domaine avec Windows 7 et Outlook 2013

2.2) Etapes d'installation

Veuillez suivre les étapes 2.3 du Scénario 2 pour les détails et les précisions. Ne sont listées ici que les différences

2.3) Configuration Exchange

2.3.1) Configuration réception des mails

Procédure :http://www.techieshelp.com/setup-exchange-2013-receive-connector/

Eléments de configuration importants pour les connecteurs à modifier (Exch01):
Ne concerne que les connecteurs de Exch01. Exch02 est similaire. Il n'y a qu'à modifier l'IP pour le network binding (192.168.1.15 au lieu de 192.168.1.14) et le FQDN (exch02.interne2.gelit.ch au lieu de exch01.interne2.gelit.ch).

Connecteur 1 : Default FrontEnd Exch01

- Sécurité
  - Authentification : TLS (permet de chiffrer la connexion entre serveurs SMTP grâce à ESMTP)
    - Concerne les connexions : Serveurs mail publics –-> CAS de Exch01
  - Permissions : Anonymous Users (tous les serveurs SMTP peuvent s'y connecter)
- Scoping :
  - Remote network settings : IPv4 : 0.0.0.0-255.255.255.255 et IPv6 : ::-ffff :ffff :ffff :ffff :ffff :ffff :ffff :ffff (permet de recevoir les mails de n'importe quel serveur SMTP)
  - Network adapter bindings : 192.168.1.14 :25 (permet de lier cette configuration à cette IP (Exch01))

Connecteur 2 : Outbound Proxy Frontend Exch01

- Sécurité
  - Authentification: TLS (authentification mutuelle), Exchange server authentification
    - Concerne les connexions : MBX –-> CAS
  - Permissions : Exchange servers
- Scoping :
  - Remote network settings : 192.168.1.14 - 192.168.1.15 (accepte les connexions provenant du rôle MBX de Exch01 et Exch02 à destination des CASs)
  - Network adapter bindings : 192.168.1.14 :717 (permet de lier cette configuration à cette IP (Exch01))
  - FQDN transmis lors de HELO/EHLO : Exch01.interne2.gelit.ch

Connecteur 3 : Default Exch01

- Sécurité
  - Authentification: TLS (authentification mutuelle), Exchange server authentification
    - Concerne les connexions : CAS –-> MBX
  - Permissions : Exchange servers
- Scoping :
  - Remote network settings : 192.168.1.14 - 192.168.1.15 (accepte les connexions provenant du rôle CAS de Exch01 et Exch02 à destination des MBXs)
  - Network adapter bindings : 192.168.1.14 :2525 (permet de lier cette configuration à cette IP (Exch01))
  - FQDN transmis lors de HELO/EHLO : Exch01.interne2.gelit.ch

2.3.2) Configuration émission des mails

http://www.techieshelp.com/exchange-2013-send-connector-configuration/

Eléments de configuration à remplacer :

- Nom : Send
- Utiliser les MX records
- Domaine : * (afin de pouvoir envoyer à tous les domaines)
- Serveurs de source : Exch01 et Exch02

Une fois le connecteur créé, il faut encore le modifier :

- Dans l'onglet général : cocher le *« Proxy through CAS »*
- Dans Scoping : FQDN : mail.gelit.ch

2.3.3) Configuration du DAG

Il faut maintenant mettre en place le DAG (Database Availability Group) afin d'assurer la haute disponibilité du rôle MBX et des bases de données par le biais du service cluster Windows. Un DAG peut contenir jusqu'à 16 serveurs Exchange et jusqu'à 100 bases de données (actives / passives) par serveur. Dans les cas où cela est possible, les serveurs Exchange devraient posséder une deuxième carte réseau. Celle-ci serait connectée à un réseau séparé pour la réplication afin d'éviter des problèmes de performance si le trafic (client/réplication) est trop important. Dans ce projet, il n'y a qu'un seul réseau pour assurer les connexions clients et le processus de réplication.

Introduction au DAG
http://exchangeserverpro.com/exchange-server-2013-database-availability-groups/

Procédure de configuration du DAG
http://exchangeserverpro.com/installing-an-exchange-server-2013-database-availability-group/
Eléments de configuration à remplacer
Cluster Name Object (CNO) = ExchDAG
DAG Name = ExchDAG
Witness Directory = none entered. Automatically chosen by Exchange = (le dossier DAGFileShareWitnesses sera crée dans le C:\)
Witness Server = FSW
DAG IP Address = 192.168.1.17

Il est possible qu'une fois la configuration effectuée, et après simulation d'une panne d'un serveur Exchange en débranchant la prise réseau, un problème ne survienne. Le cluster et la base de données peuvent tomber en panne si le FSW au niveau du cluster est mal mis en place.

Il est possible que la mise en place du FSW échoue, même si :

- Le cluster est bien mis en place

- Exchange est bien configuré pour l'utilisation du FSW
- Le dossier de partage sur le FSW a bien été créé mais, que le cluster et la base de données tombent lorsqu'un serveur est débranché .

Le problème peut être au niveau du cluster et le FSW n'y est pas présent.
Dans ce cas, il faut :

- Vérifier que le dossier sur le FSW a bien été créé sur le C:\
- Partager manuellement le dossier pour l'accès complet aux administrateurs
- Ouvrir le « Failover Cluster Manager » de Windows Server 2012
- Se connecter sur le cluster
- Cliquer sur : ExchDAG.interne2.gelit.ch
- Vérifier dans la partie « Cluster Core Ressources » que le FSW est bien présent. S'il n'est pas présent :
    - Clique droit sur le Cluster – More Actions – Configure Cluster Quorum Settings
    - Select the Quorum Witness – Configure a FSW
    - File Share Path : \\FSW\DAGFileShareWitnesses

Une fois terminé, le FSW devrait être visible et le cluster rester en vie si un des serveurs Exchange tombe en panne.

Procédure de configuration des copies de bases de données
http://exchangeserverpro.com/exchange-2013-dag-database-copies/

Démo de l'utilisation du Quorum Windows avec le DAG
http://exchangeserverpro.com/windows-server-2012-dynamic-quorum/

Détails supplémentaires sur la configuration du Quorum (pas nécessaire pour cette configuration)
http://technet.microsoft.com/en-us/library/jj612870.aspx

2.3.4) Certificats Serveurs CAS

Pour les informations de base et la procédure à suivre, se référer au 2.4.10, Scénario 1 pour le serveur Exch01.
Une fois que les étapes décrites dans le 2.4.10 ont bien été effectuées et que le certificat a été installé sur Exch01, il faut exporter le certificat créé, mais uniquement en passant par la console Exchange et non par une MMC. Une fois exporté, le certificat doit être importé pour Exch02.
http://exchangeserverpro.com/exchange-2013-ssl-certificate-export-import/

2.3.5) Configuration pfSense pour le Failover

2.3.5.1) Règles de pare-feu

Configuration des alias

Firewall: Aliases

Name	Values	Description
CAS_ports	25, 443	1
ExchDAG_hosts	192.168.1.14, 192.168.1.15	2

Figure 9 : Alias

Ces alias permettront de regrouper certaines règles de pare-feu.

Configuration des règles (interface WAN)

Firewall: Rules

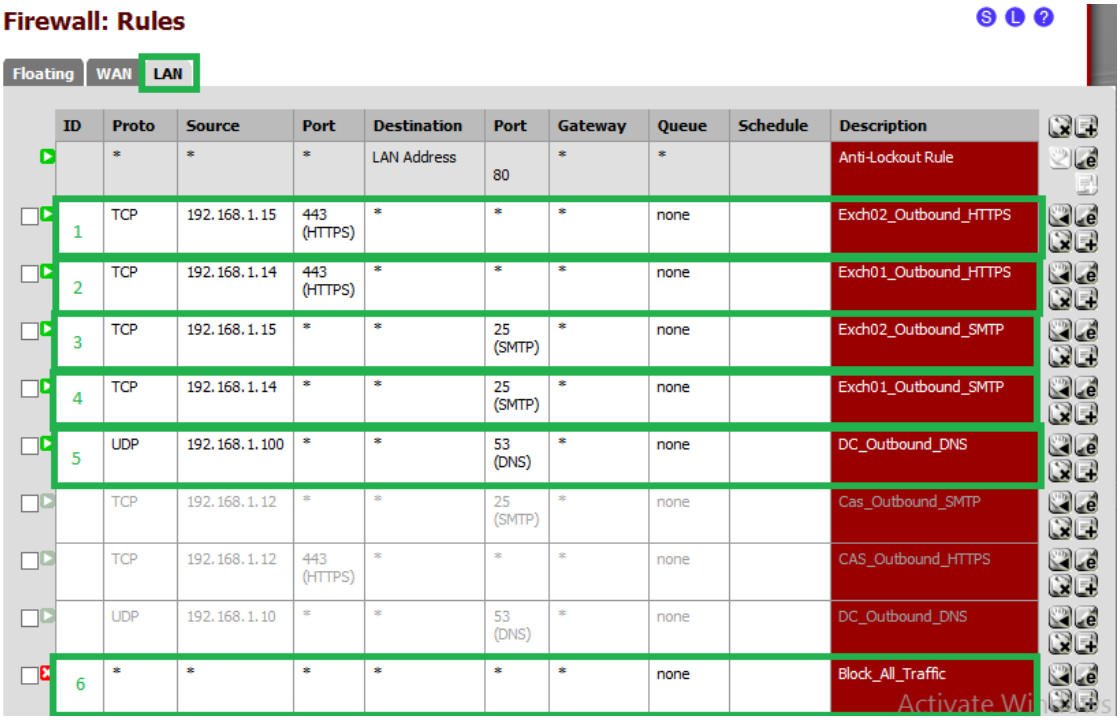
Floating | WAN | LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	RFC 1918 networks	*	*	*	*	*		Block private networks
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
	1	UDP	*	*	192.168.1.100	53 (DNS)	*	none		Inbound_DNS
	2	TCP	*	*	ExchDAG_hosts	CAS_ports	*	none		ExchDAG
		UDP	*	*	192.168.1.10	53 (DNS)	*	none		DC_Inbound_DNS
		TCP	*	*	192.168.1.12	25 (SMTP)	*	none		NAT Redirect_SMTP
		TCP	*	*	192.168.1.12	443 (HTTPS)	*	none		NAT Redirect_HTTPS
	3	*	*	*	*	*	*	none		Block_All_Traffic

Figure 10 : WAN Inbound Rules

1) Autorise le trafic DNS entrant en réponse à une requête du DNS
2) Autorise le trafic HTTPS/SMTP entrant à destination de Exch01 et 2
3) Bloque tout le reste du trafic

Configuration des règles (interface LAN)



ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
1	TCP	192.168.1.15	443 (HTTPS)	*	*	*	none		Exch02_Outbound_HTTPS
2	TCP	192.168.1.14	443 (HTTPS)	*	*	*	none		Exch01_Outbound_HTTPS
3	TCP	192.168.1.15	*	*	25 (SMTP)	*	none		Exch02_Outbound_SMTP
4	TCP	192.168.1.14	*	*	25 (SMTP)	*	none		Exch01_Outbound_SMTP
5	UDP	192.168.1.100	*	*	53 (DNS)	*	none		DC_Outbound_DNS
	TCP	192.168.1.12	*	*	25 (SMTP)	*	none		Cas_Outbound_SMTP
	TCP	192.168.1.12	443 (HTTPS)	*	*	*	none		CAS_Outbound_HTTPS
	UDP	192.168.1.10	*	*	53 (DNS)	*	none		DC_Outbound_DNS
6	*	*	*	*	*	*	none		Block_All_Traffic

Figure 11 : LAN Outbound Rules

1) Autorise le trafic sortant HTTPS de Exch02 en réponse à une requête entrante d'un client
2) Autorise le trafic sortant HTTPS de Exch01 en réponse à une requête entrante d'un client
3) Autorise le trafic sortant SMTP de Exch02
4) Autorise le trafic sortant SMTP de Exch01
5) Autorise le trafic DNS sortant du service DNS du DC
6) Bloque tout le trafic restant

2.3.5.2) Failover

Le Failover permet d'assurer la haute disponibilité pour le rôle CAS.
Voici la procédure pour un serveur WEB, mais elle est similaire pour Exchange.
http://pfsensesetup.com/pfsense-load-balancing-part-three-web-server-failover/

La configuration voulue est la suivante :

- Les connexions SMTP / HTTPS entrantes sont dirigées vers Exch01
- Si le serveur Exch01 tombe en panne, toutes les connexions sont redirigées vers Exch02
- Lorsque Exch01 est disponible à nouveau, les connexions y retournent.
- Si le service HTTPS est indisponible pour Exch01, alors elles sont redirigées vers Exch02. Si le service SMTP de Exch01 est toujours fonctionnel, alors les connexions SMTP restent dirigées vers Exch01
- Les connexions sont donc gérées en fonction de la disponibilité des services et non de celle des serveurs

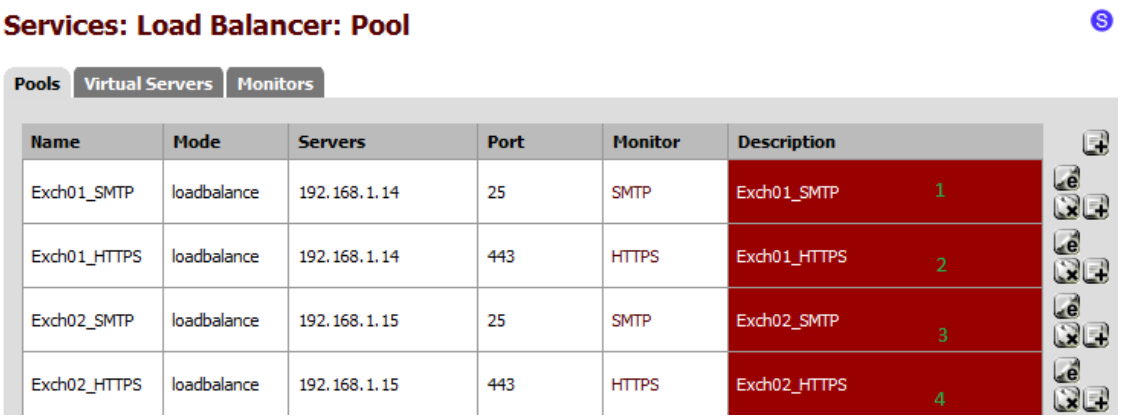


Figure 12 : Load Balancer Pool

Chacun des services de chaque serveur est considéré comme un pool. Cela permet d'avoir un failover basé sur la disponibilité des services et non de celle des serveurs.
La partie « Monitor » définit quels services sont surveillés par pfSense pour vérifier la disponibilité des services en initiant des connexions SMTP et HTTPS sur les deux serveurs régulièrement.

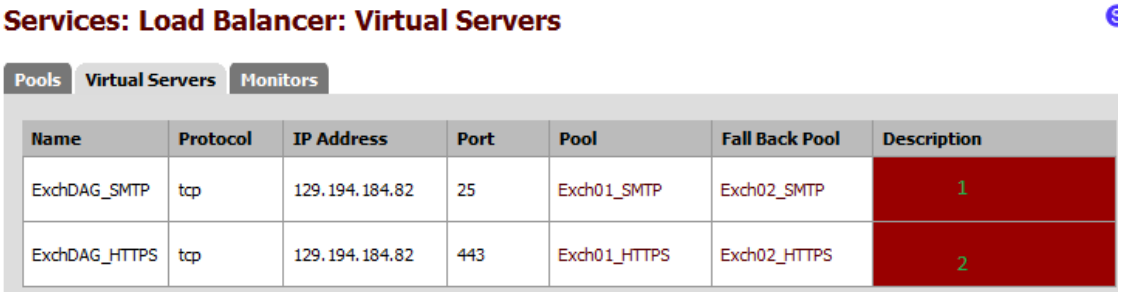


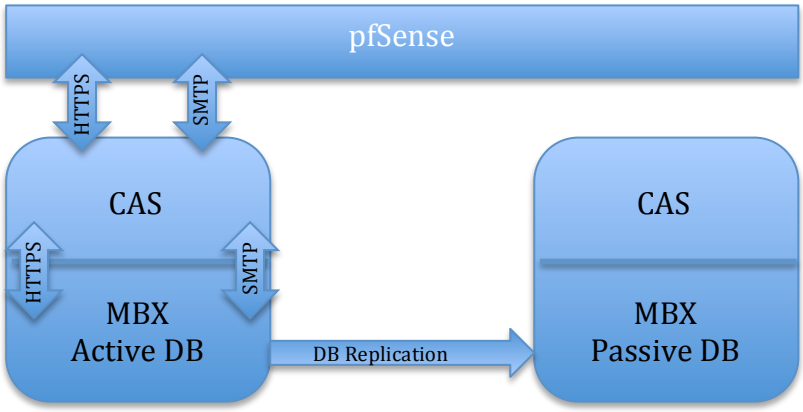
Figure 13 : Virtual Servers

Dans cet onglet, on remarque que deux serveurs virtuels ont été configurés (car il y a deux services, HTTPS et SMTP). Seuls les services de Exch01 apparaissent dans le pool principal ce qui définit Exch01 comme serveur principal. Les services de Exch02 sont utilisés comme « Fall Back Pool », ce qui définit Exc02 comme serveur de secours.

III/ Test

3.1) Situation initiale

Dans ce cas, les serveurs et leurs services fonctionnent correctement.



Exch01 Exch02

Status: Load Balancer: Pool

Pools | Virtual Servers

Name	Mode	Servers	Monitor	Description
Exch01_SMTP	Load balancing	192.168.1.14:25 (98.22%)	SMTP	Exch01_SMTP
Exch01_HTTPS	Load balancing	192.168.1.14:443 (98.72%)	HTTPS	Exch01_HTTPS
Exch02_SMTP	Load balancing	192.168.1.15:25 (98.91%)	SMTP	Exch02_SMTP
Exch02_HTTPS	Load balancing	192.168.1.15:443 (99.54%)	HTTPS	Exch02_HTTPS

Tous les services des deux serveurs sont opérationnels

NAME	ACTIVE ON SERVER	SERVERS WITH C...	STATUS
Database1	EXCH01	EXCH01,EXCH02	Mounted

La copie de la DB est active sur Exch01

Status: System logs: Firewall

System | Firewall | DHCP | Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | OpenNTPD | Wireless | Settings

Normal View | Dynamic View | Summary View

1 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	Jun 23 09:20:46	WAN	212.82.97.135:27299	192.168.1.14:25	TCP:S

Les connexions SMTP entrantes/sortantes sont bien redirigées vers Exch01

Status: System logs: Firewall

System | Firewall | DHCP | Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | OpenNTPD | Wireless | Settings

Normal View | Dynamic View | Summary View

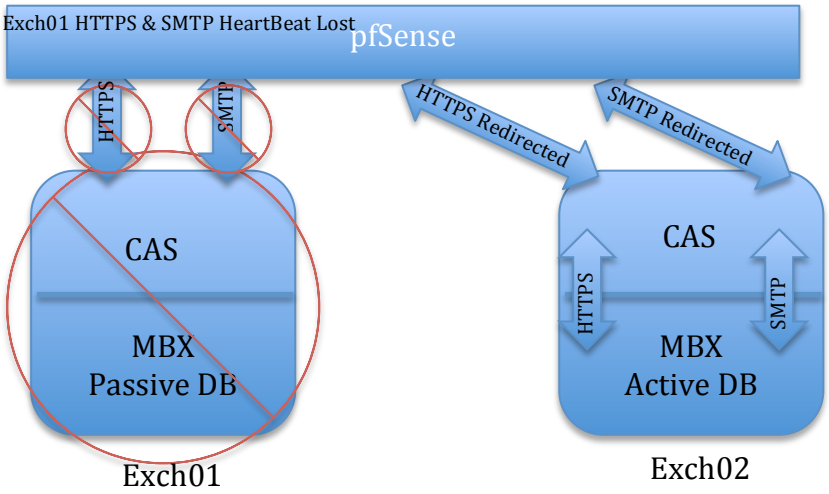
4 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	Jun 23 09:20:26	WAN	213.55.176.139:35507	192.168.1.14:443	TCP:S

Les connexions HTTPS entrantes/sortantes sont bien redirigées vers Exch01

3.2) Simulation de panne Exch01

Dans ce test, on simule une panne complète de Exch01 en retirant la prise Ethernet. PfSense diagnostique une panne des services HTTPS et SMTP de Exch01 grâce aux monitors et redirige les requêtes vers Exch02. Le cluster diagnostique la panne du serveur Exch01 et Exchange active la DB de Exch02



Status: Load Balancer: Pool

Pools | Virtual Servers

Name	Mode	Servers	Monitor	Description
Exch01_SMTP	Load balancing	192.168.1.14:25 (98.21%)	SMTP	Exch01_SMTP
Exch01_HTTPS	Load balancing	192.168.1.14:443 (98.71%)	HTTPS	Exch01_HTTPS
Exch02_SMTP	Load balancing	192.168.1.15:25 (98.91%)	SMTP	Exch02_SMTP
Exch02_HTTPS	Load balancing	192.168.1.15:443 (99.54%)	HTTPS	Exch02_HTTPS

Les services HTTPS et SMTP de Exch01 sont hors service

NAME	ACTIVE ON SERVER	SERVERS WITH C...	STATUS	B...
Database1	EXCH02	EXCH01,EXCH02	Mounted	0

La DB devient active sur Exch02

1 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	Jun 23 09:30:38	WAN	212.82.97.112:38355	192.168.1.15:25	TCP:S

Les connexions SMTP entrantes/sortantes sont bien redirigées vers Exch02

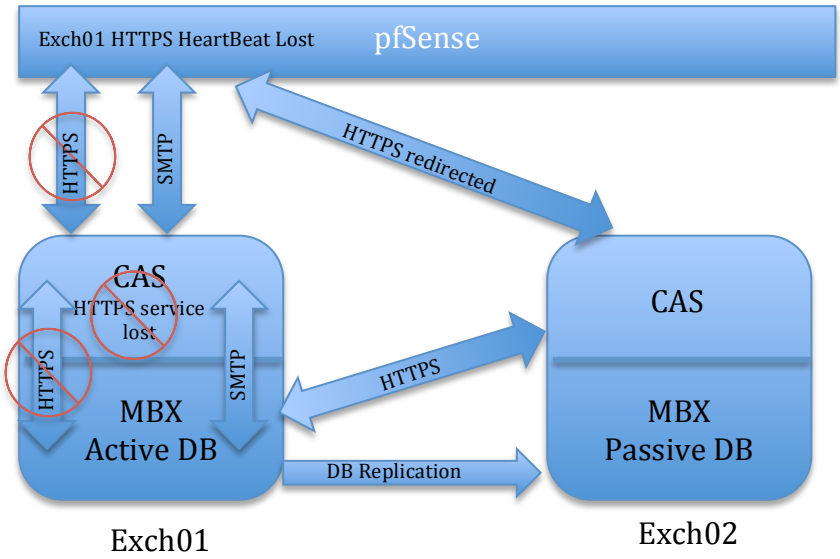
1 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	Jun 23 09:30:34	WAN	213.55.176.139:32428	192.168.1.15:443	TCP:S

Les connexions HTTPS entrantes/sortantes sont bien redirigées vers Exch02

3.3) Simulation de panne HTTPS Exch01

Pour cela, on stoppe IIS de Exch01



Status: Load Balancer: Pool

Pools | Virtual Servers

Name	Mode	Servers	Monitor	Description
Exch01_SMTP	Load balancing	192.168.1.14:25 (98.00%)	SMTP	Exch01_SMTP
Exch01_HTTPS	Load balancing	192.168.1.14:443 (98.48%)	HTTPS	Exch01_HTTPS
Exch02_SMTP	Load balancing	192.168.1.15:25 (98.92%)	SMTP	Exch02_SMTP
Exch02_HTTPS	Load balancing	192.168.1.15:443 (99.54%)	HTTPS	Exch02_HTTPS

Le service HTTPS de Exch01 est indisponible pour pfSense

NAME	ACTIVE ON S...	SERVERS WITH COPIES	STATUS
Database1	EXCH01	EXCH01,EXCH02	Mounted

La DB est toujours active sur Exch01

1 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	Jun 23 09:42:20	WAN	212.82.97.139:23264	192.168.1.14:25	TCP:S

Les connexions SMTP entrantes/restantes restent dirigées vers Exch01

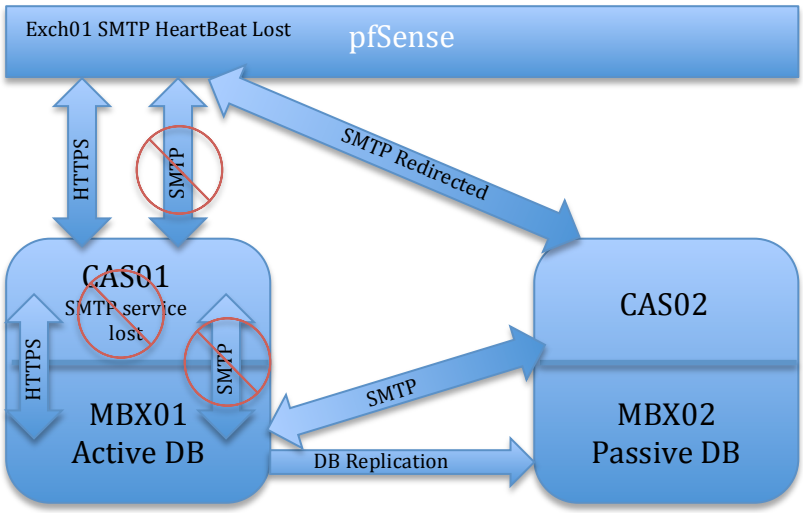
2 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	Jun 23 09:42:13	WAN	213.55.176.139:34628	192.168.1.15:443	TCP:S
	Jun 23 09:43:18	WAN	213.55.176.139:32950	192.168.1.15:443	TCP:S

Les connexions HTTPS entrantes/sortantes sont maintenant dirigées vers Exch02

3.4) Service SMTP indisponible sur Exch01

Afin de bloquer le service SMTP d'Exchange, on stoppe le service « Microsoft Exchange Frontend Transport »



Status: Load Balancer: Pool

Pools | Virtual Servers

Name	Mode	Servers	Monitor	Description
Exch01_SMTP	Load balancing	192.168.1.14:25 (44.55%)	SMTP	Exch01_SMTP
Exch01_HTTPS	Load balancing	192.168.1.14:443 (80.00%)	HTTPS	Exch01_HTTPS
Exch02_SMTP	Load balancing	192.168.1.15:25 (100.00%)	SMTP	Exch02_SMTP
Exch02_HTTPS	Load balancing	192.168.1.15:443 (100.00%)	HTTPS	Exch02_HTTPS

Le service SMTP de Exch01 est bien indisponible

NAME	ACTIVE ON SERVER	SERVERS WITH C...	STATUS
Database1	EXCH01	EXCH01,EXCH02	Mounted

La DB est toujours active sur Exch01

Act	Time	If	Source	Destination	Proto
	Jun 23 11:52:06	LAN	192.168.1.15:7140	188.125.69.79:25	TCP:SEW
	Jun 23 11:48:53	LAN	192.168.1.15:6814	216.32.181.178:25	TCP:SEW
	Jun 23 11:48:54	WAN	212.82.96.124:20135	192.168.1.15:25	TCP:S

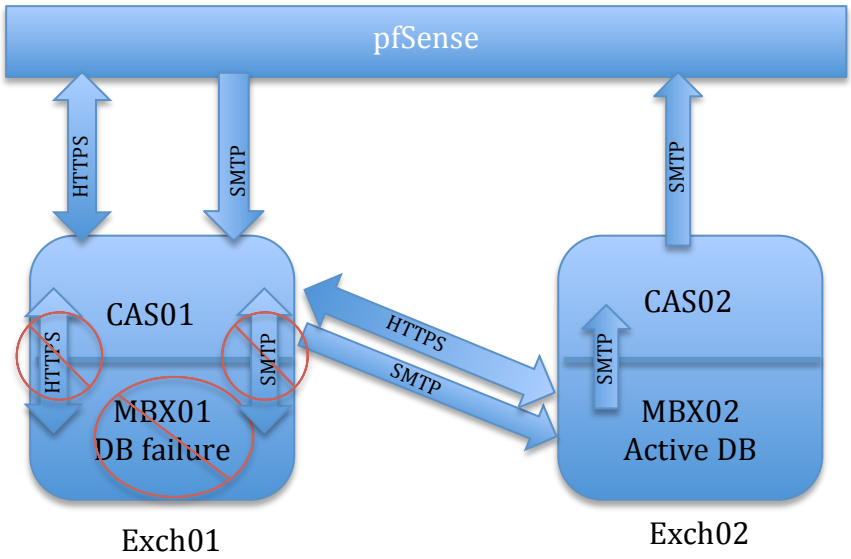
Les connexions SMTP entrantes/sortantes passent par Exch02

	Jun 23 11:50:39	WAN	213.55.176.243:35664	192.168.1.14:443	TCP:S

Les connexions HTTPS entrantes/sortantes passent toujours par Exch01

3.5) Simulation de panne de Base de données Exch01

Pour cela, on stoppe le service « Microsoft Exchange Information Store » de Exch01. La DB ne sera plus active sur ce serveur.



Status: Load Balancer: Pool

Pools | Virtual Servers

Name	Mode	Servers	Monitor	Description
Exch01_SMTP	Load balancing	192.168.1.14:25 (98.22%)	SMTP	Exch01_SMTP
Exch01_HTTPS	Load balancing	192.168.1.14:443 (98.72%)	HTTPS	Exch01_HTTPS
Exch02_SMTP	Load balancing	192.168.1.15:25 (98.91%)	SMTP	Exch02_SMTP
Exch02_HTTPS	Load balancing	192.168.1.15:443 (99.54%)	HTTPS	Exch02_HTTPS

Tous les services sont disponibles. Toutes les connexions entrantes vont sur Exch01

NAME	ACTIVE ON SERVER	SERVERS WITH C...	STATUS	B...
Database1	EXCH02	EXCH01,EXCH02	Mounted	0

La DB est bien active sur Exch02

Act	Time	If	Source	Destination	Proto
	Jun 23 11:01:32	LAN	192.168.1.15:59836	188.125.69.79:25	TCP:SEW

Connexions SMTP sortantes par Exch02
Connexions SMTP entrantes par Exch01

	Jun 23 11:00:46	WAN	213.55.176.243:35075	192.168.1.14:443	TCP:S

Connexions entrantes/sortantes HTTPS passent par Exch01

IV/ Scénario sans LB

Ce scénario se concentre sur un niveau de disponibilité moyen (par rapport au scénario précédent) en passant par une disponibilité de type Round Robin DNS pour les communications clientes HTTPS et par la mise en place d'un deuxième record MX pour les communications SMTP entre serveurs.

4.1) Analyse

4.1.1) DNS Round Robin

Le DNS Round Robin est un mécanisme qui, au niveau du serveur DNS, permet de lier plusieurs IPs à un FQDN pour permettre la répartition de charge. Ce n'est en aucun cas un système de tolérance de pannes. En effet, il n'y a aucune détection de panne de service pour le serveur de destination. Le serveur DNS ainsi que le client doivent supporter une telle configuration.
En ce qui concerne le client, comment gère-t-il le Round Robin ? Selon Microsoft, un Windows Vista ne se comporte pas de la même manière qu'un Windows 7[12]. Mais le « switching » d'adresse est géré par un « timer ». Il est de 15 minutes pour un Windows 7 et de 1 minute pour un serveur 2012 R2. Le choix de l'IP par l'OS ne sera pas lié au TTL.
Quel est le risque d'un tel système ?
Si un client est connecté au server Exch01 et que ce dernier tombe en panne, le client aura une connexion dégradée pendant 15 minutes.
Une fois que le client pourra se connecter à la seconde adresse pointant sur Exch02 à la fin des 15 minutes, la connectivité sera bonne mais ne sera que temporaire. En effet, au bout de ces 15 minutes, le client utilisera de nouveau l'IP pointant sur Exch01, qui peut toujours être indisponible créant donc ainsi une autre dégradation de service.
Un autre risque concerne l'aspect aléatoire du RR pour un client. Il y a des « timers » différents selon les OS ou éventuellement d'autres modes de fonctionnement.
Au final, afin d'assurer une véritable disponibilité avec un tel système, l'administrateur doit retirer l'entrée DNS du serveur en panne manuellement afin d'éviter une redirection inutile des connexions à sa destination.

4.1.2) Backup MX

L'utilité d'un Backup MX est de constituer un chemin de secours si le serveur de messagerie principale (Exch01) tombe en panne (ou son service SMTP). Le serveur ayant ici la priorité la plus élevée est le Exch01 atteignable par : 129.194.184.82. Le serveur ayant la priorité moindre est Exch02, atteignable par : 129.194.184.88. Par défaut, lorsqu'un serveur de messagerie voudra envoyer un mail à gelit.ch, il choisira le record MX ayant la valeur la plus basse (Exch01). Si le serveur émetteur, trouve le serveur Exch01 indisponible, il essaye immédiatement le chemin par le Backup MX passant par Exch02.

[12] http://support.microsoft.com/kb/968920

4.2) Cahier des charges

Identique au 2.1 du scénario 3, avec en plus :

- Utilisation d'une deuxième IP publique : 129.194.184.88
- FQDN supplémentaire pour les connexions clients : owa.gelit.ch
- Deuxième firewall pfSense pour la deuxième IP
- Second record MX

4.3) Topologie physique

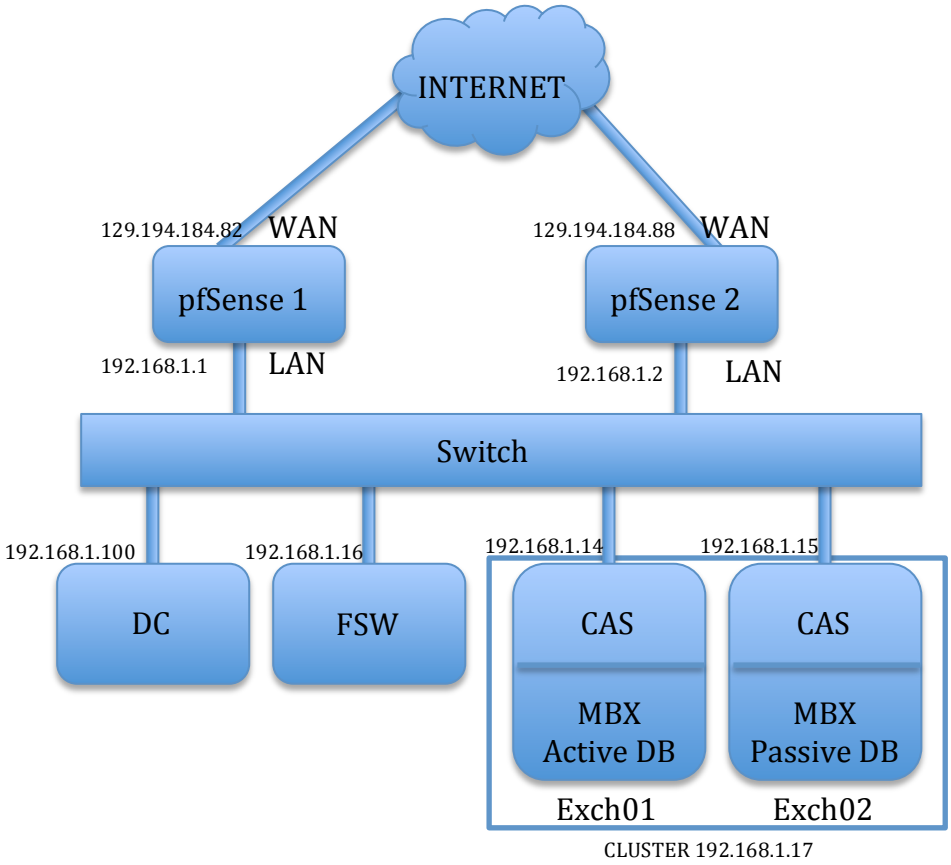


Figure 14 : Topologie physique

4.4) Principe de fonctionnement

Dans le cadre du Round Robin avec un client Outlook 2013, l'IP de destination véritable dépend directement de l'ordre des adresses IPs dans le cache DNS du client pour owa.gelit.ch. Ici, je suppose que les connexions clients sont à destination des deux serveurs car l'ordre des IPs pour les deux clients est inversé.
Lorsque tous les serveurs sont en ligne, tout le trafic est à destination de la première IP du cache. En cas de panne du serveur avec l'IP principale présente dans le cache, les paquets iront à destination des IP principale et secondaire à la fois. En effet, les clients tenteront toujours de se reconnecter au serveur possédant l'IP principale (la première affichée dans le cache) et, s'ils n'y arrivent pas, il transmettent les paquets également au serveur possédant l'IP secondaire ce qui rend le temps de connexion plus long. Sur les schémas cela s'appelle mode dégradé

4.4.1) Schéma HTTPS

Légende

Connexion Client 1 > IP principale sur Exch01

Connexion Client 2 > IP secondaire sur Exch02

mode dégradé

Fonctionnement normal

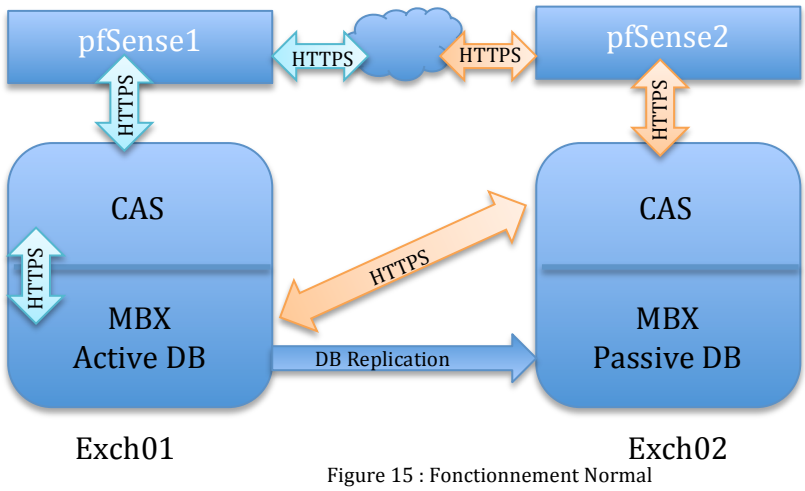


Figure 15 : Fonctionnement Normal

Le client 1 se connecte sur Exch01 (première IP dans son cache DNS)
Le client 2 se connecte sur Exch02 (première IP dans son cache DNS)

Service HTTPS de Exch01 indisponible

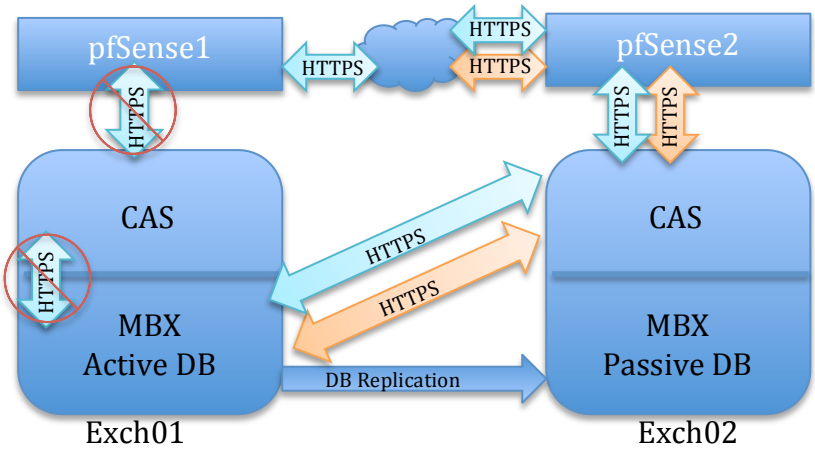


Figure 16 : Panne HTTPS Exch01

Le client 1 perd la connexion sur le serveur Exch01 pour 15 minutes maximum. Une partie des paquets tente de joindre Exch01, et l'autre partie se dirige sur Exch02 (mode dégradé).
Le client 2 garde la connexion pour 15 minutes maximum.
Après 15 minutes, il y a switching d'IP. Dans ce cas :
Le client 2 passe par Exch01 et est donc en mode dégradé pour 15 minutes maximum.
Le client 1 passe par Exch02 et reprend la connexion pour 15 minutes maximum

Exch01 indisponible

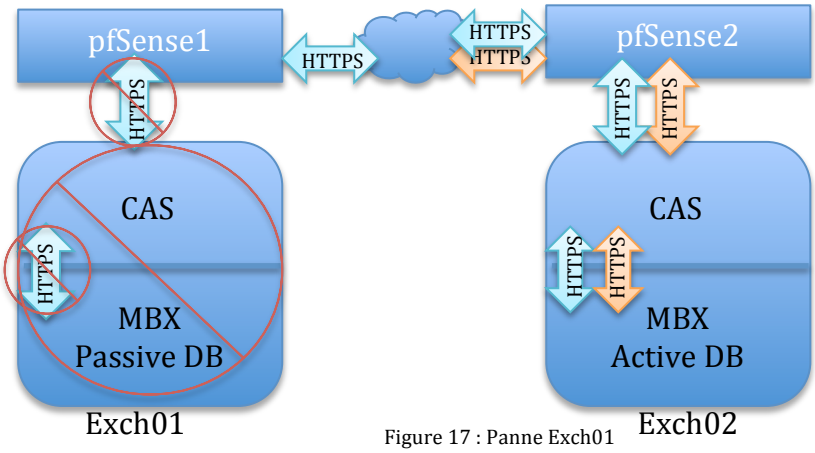


Figure 17 : Panne Exch01

Le client 1 perd la connexion sur le serveur Exch01 pour 15 minutes maximum. Une partie des paquets tente de joindre Exch01, et l'autre partie se dirige sur Exch02 (mode dégradé).
Le client 2 garde la connexion pour 15 minutes maximum.
Après 15 minutes, il y a le switching d'IP. Dans ce cas :
Le client 2 passe par Exch01 et est donc en mode dégradé pour 15 minutes maximum.
Le client 1 passe par Exch02 et reprend la connexion pour 15 minutes maximum.
Le scénario est similaire pour Exch02, s'il lui ou son service HTTPS devenait indisponible.

4.4.2) Schéma SMTP

Légende

Connexion SMTP avec MX primaire

Connexion SMTP avec MX Secondaire

Connexion perdue

Fonctionnement normal

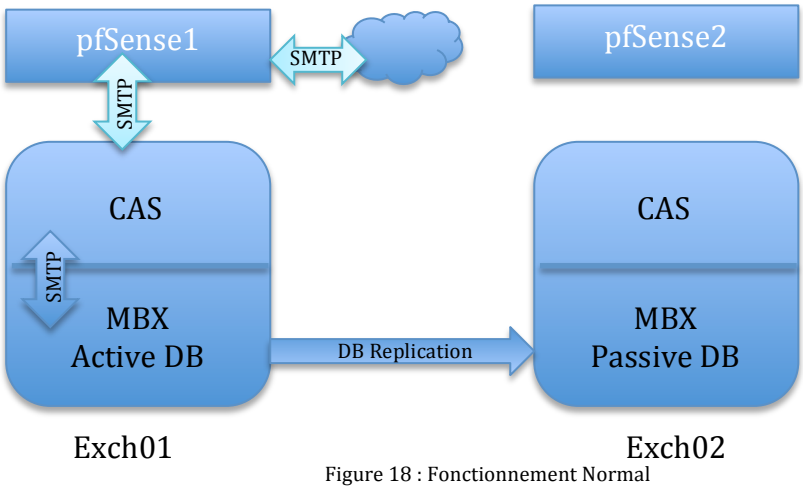


Figure 18 : Fonctionnement Normal

Service SMTP de Exch01 indisponible

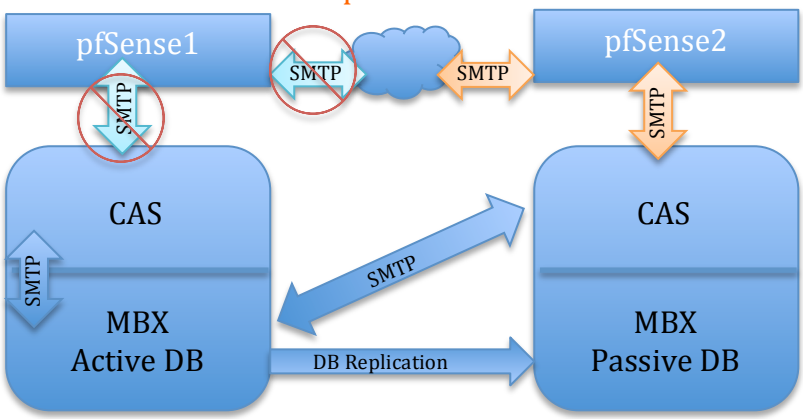


Figure 19 : Panne SMTP Exh01

Exch01 indisponible

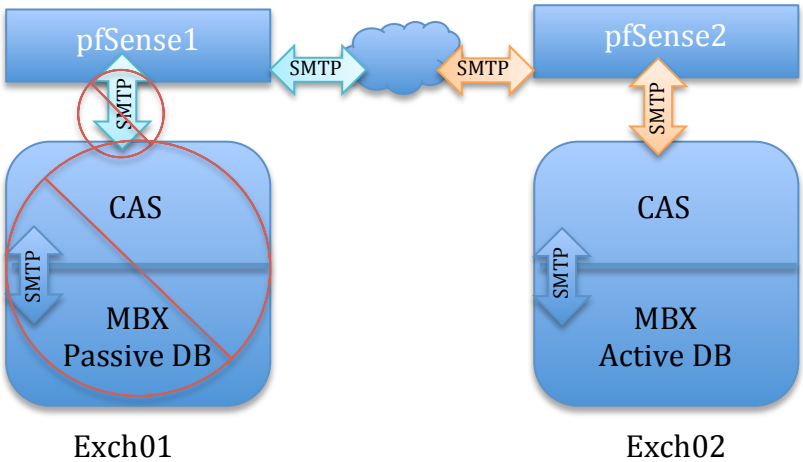


Figure 20 : Panne Exch01

A chaque tentative de connexion SMTP par un serveur de messagerie externe, ce dernier tentera d'établir une connexion SMTP en passant par le MX principal pointant sur Exch01. Si Exch01, ou son service SMTP, est indisponible, alors le serveur de messagerie externe utilisera le MX secondaire pointant sur Exch02.

4.5) Configuration

4.5.1) Configuration DNS

Pour mettre en place le DNS RR, il est nécessaire d'avoir deux IPs pour le même FQDN. Etant donné que cette configuration n'est nécessaire que pour les connexions clientes dans ce scénario, il y a un nouveau FQDN : owa.gelit.ch. Les clients utiliseront ce nouveau FQDN pour Outlook et l'OWA. Seules les connexions HTTPS seront redirigées par ce mécanisme entre Exch01 et Exch02
Pour les connexions SMTP, un deuxième MX de priorité inférieure est mis en place pour la redirection des connexions. Si Exch01 ne répond plus sur le port 25, les serveurs de messagerie externes utiliseront le deuxième MX.

Hostname	Type	Priority	Target(IP or Host)
mail2.gelit.ch.	A		129.194.184.88
gelit.ch.	MX	20	mail2.gelit.ch
owa.gelit.ch.	A		129.194.184.88
owa.gelit.ch.	A		129.194.184.82
gelit.ch.	A		129.194.184.82
autodiscover.gelit.ch.	A		129.194.184.82
gelit.ch.	MX	10	mail.gelit.ch
mail.gelit.ch.	A		129.194.184.82

Figure 21 : Contenu DNS Public

4.5.2) Configuration Exchange

En ce qui concerne Exchange, il est important de changer les « external URLs » des « Virtual Directories ». Ils étaient configurés pour mail.gelit.ch précédemment, mais il faut maintenant les remplacer par owa.gelit.ch. Cela permettra aux clients de récupérer la bonne configuration par l'autodiscovery. Il faut également rajouter le FQDN owa.gelit.ch dans le certificat de Exch01 et Exch02.
Voici un exemple pour l'OWA:

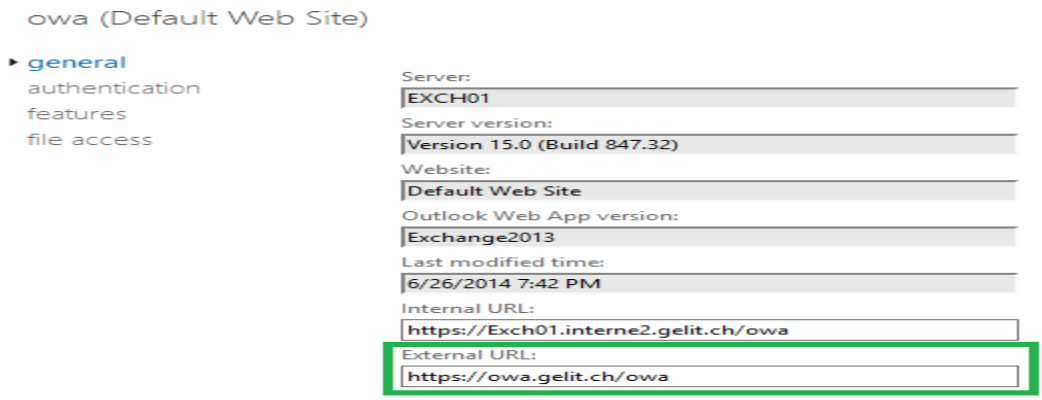


Figure 22 : Configuration URL OWA pour l'Autodiscover

4.5.3) Configuration pfSense

Il y a maintenant 2 serveurs pfSense pour deux IPs. Le premier est responsable de l'adresse 129.194.184.82 et le deuxième pour la 129.194.184.88.
Les changements dans le firewall sont pour les connexions entrantes.

Voici la configuration pour le pfSense 1 :

Configuration NAT

	WAN	TCP	*	*	WAN address	25 (SMTP)	192.168.1.14	25 (SMTP)	Allow_inbound_CAS1_SMTP
	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.1.14	443 (HTTPS)	Allow_inbound_CAS1_HTTPS

Figure 23 : Configuration NAT pfSense 1

Redirection des ports SMTP et HTTPS pour Exch01 avec 129.194.184.82

Configuration Firewall

		TCP	*	*	192.168.1.14	25 (SMTP)	*	none		NAT Allow_inbound_CAS1_SMTP
		TCP	*	*	192.168.1.14	443 (HTTPS)	*	none		NAT Allow_inbound_CAS1_HTTPS

Figure 24 : Configuration Firewall pfSense 1

Autorise le trafic entrant SMTP et HTTPS pour Exch01

Voici la configuration pour le pfSense 2 :

Configuration NAT

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.1.15	443 (HTTPS)	Allow_inbound_CAS2_HTTPS
	WAN	TCP	*	*	WAN address	25 (SMTP)	192.168.1.15	25 (SMTP)	Allow_inbound_CAS2_SMTP

Figure 25 : Configuration NAT pfSense 2

Redirection des ports SMTP et HTTPS pour Exch02 avec 129.194.184.88

Configuration Firewall

		TCP	*	*	192.168.1.15	443 (HTTPS)	*	none		NAT Allow_inbound_CAS2_HTTPS
		TCP	*	*	192.168.1.15	25 (SMTP)	*	none		NAT Allow_inbound_CAS2_SMTP

Figure 26 : Configuration Firewall pfSense 2

Autorise le trafic entrant SMTP et HTTPS pour Exch02

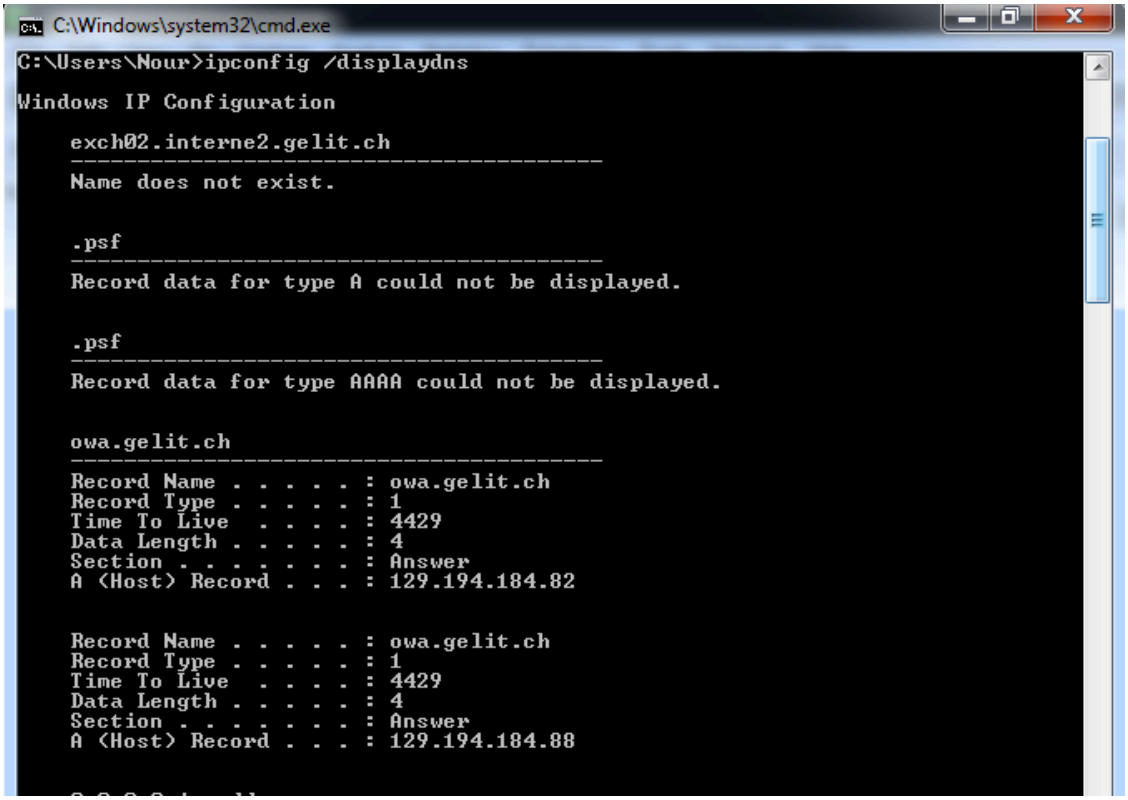
V/ Test

5.1) Test du Round Robin (fonctionnement normal)

Contexte de test :

- Exch01 et Exch02 en ligne
- DB active sur Exch01
- FQND : owa.gelit.ch
- IP principal pour le client (voir plus bas) : 129.194.184.82
- IP secondaire : 129.194.184.88

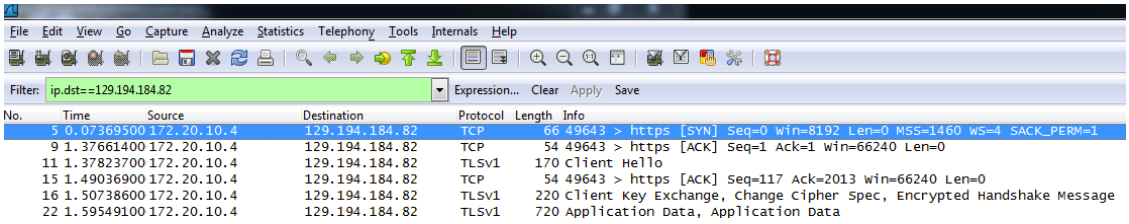
Contenu du cache DNS de Windows lors de la requête DNS pour owa.gelit.ch
Veuillez observer l'ordre des adresses pour owa.gelit.ch qui est essentiel dans la gestion des connexions.



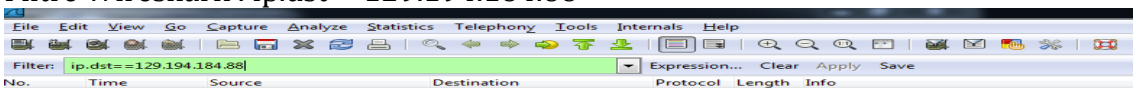
L'ordre des adresses dans le cache est essentiel car il définit la « préférence » pour la transmission des paquets. La première entrée pour owa.gelit.ch : 129.194.184.82 définit l'adresse « principale » de destination pour la transmission des paquets pour le client, tant que les 2 serveurs sont en ligne.
Si Exch01 tombe en panne, la deuxième adresse IP, 129.194.184.88 est utilisée, mais les connexions seront plus lentes. Pourquoi ?
Voir test 5.2 et 5.4

Voici des captures d'écran de Wireshark sur le PC client utilisant Outlook 2013

Filtre Wireshark : ip.dst==129.194.184.82



Filtre Wireshark : ip.dst==129.194.184.88



Dans cette situation, on peut voir que toutes les connexions passent par Exch01 et aucune par Exch02.

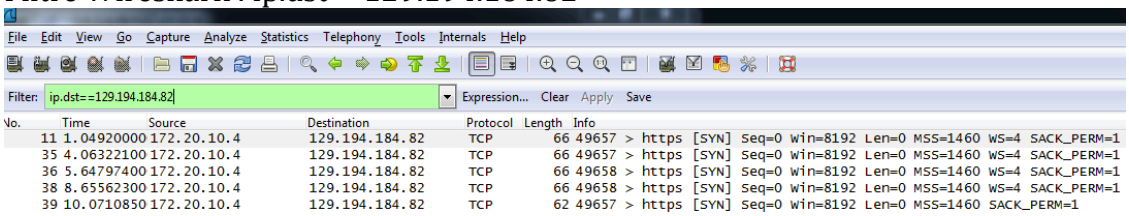
5.2) Test du Round Robin (Exch01 en panne)

Contexte de test :

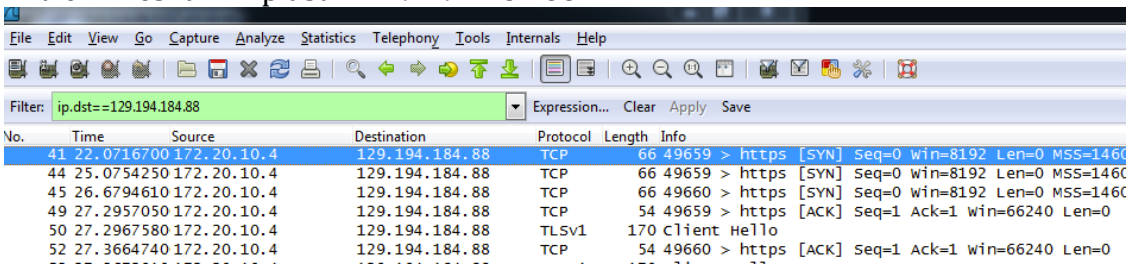
- Exch01 en panne
- Exch02 en ligne
- DB active sur Exch02
- FQND : owa.gelit.ch
- IP principale : 129.194.184.82
- IP secondaire : 129.194.184.88
- Contenu du cache DNS pareil qu'au 5.1
- Conséquence d'une telle situation ?

Voici les analyses Wireshark

Filtre Wireshark : ip.dst==129.194.184.82



Filtre Wireshark : ip.dst==129.194.184.88



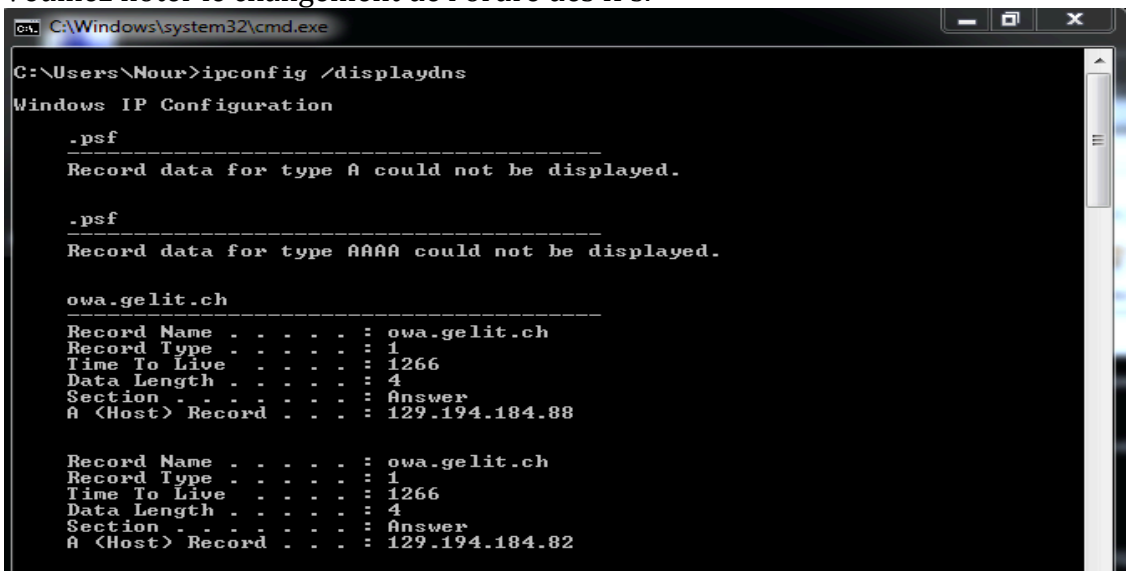
La raison pour laquelle nous retrouvons des paquets à destination des deux serveurs c'est que Exch01 est, dans le cache DNS du client, toujours considérée comme l'adresse principale. Outlook 2013 tentera tout de même d'utiliser l'adresse principale, mais sans succès. Des paquets seront toujours transmis vers Exch01 (en moins grand nombre) mais comme il n'y a aucune réponse, les paquets sont retransmis vers Exch02, ce qui explique la lenteur de la connexion de Outlook 2013 avec Exchange.

5.3) Test du Round Robin (fonctionnement normal)

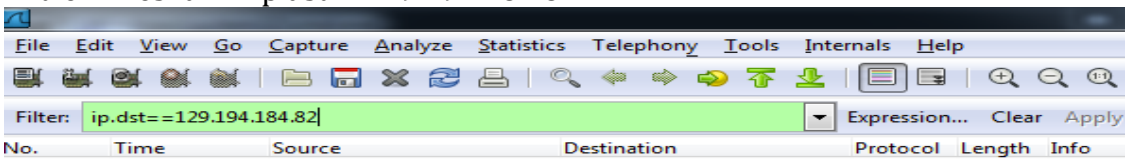
Contexte de test :

- Exch01 et Exch02 en ligne
- DB active sur Exch02
- FQND : owa.gelit.ch
- IP principale(voir plus bas) : 129.194.184.88
- IP secondaire : 129.194.184.82

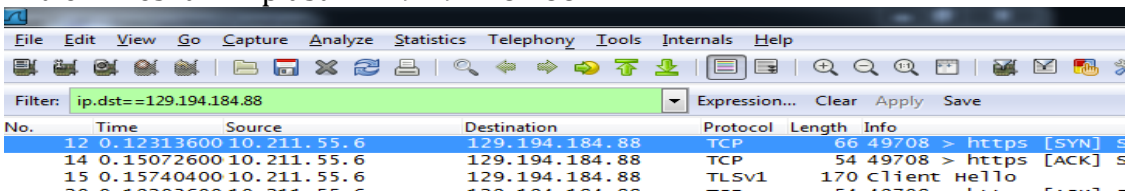
Veuillez noter le changement de l'ordre des IPs.



Filtre Wireshark : ip.dst==129.194.184.82



Filtre Wireshark : ip.dst==129.194.184.88



Veuillez noter le changement. 129.194.184.88 étant la première IP dans le cache (donc la principale maintenant) et les 2 serveurs étant bien en ligne, tous les paquets passent par Exch02.

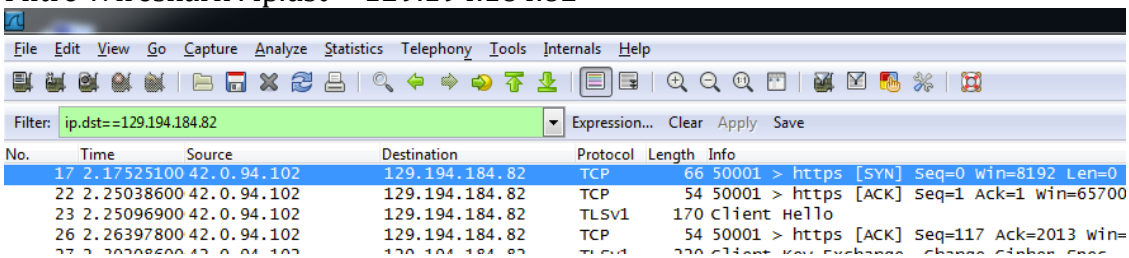
5.4) Test du Round Robin (Exch02 en panne)

Contexte de test :

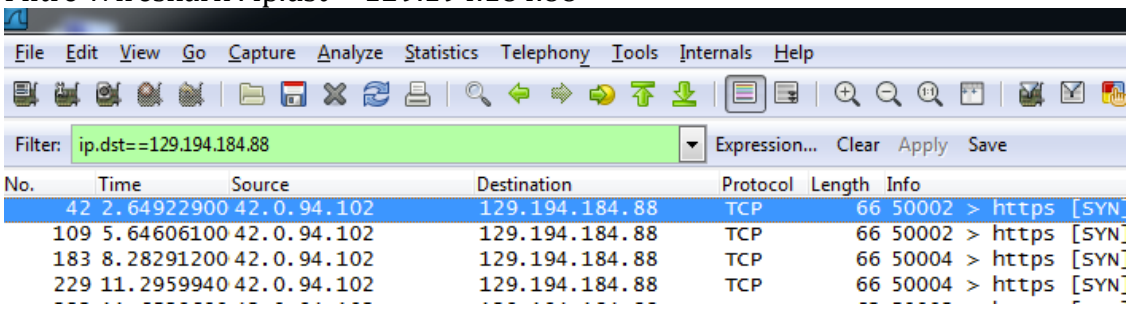
- Exch02 en panne
- Exch01 en ligne
- DB active sur Exch01
- FQND : owa.gelit.ch
- IP principale: 129.194.184.88
- IP secondaire : 129.194.184.82
- Contenu du cache DNS pareil qu'au 5.3
- Conséquence d'une telle situation ?

Voici les analyses Wireshark

Filtre Wireshark : ip.dst==129.194.184.82



Filtre Wireshark : ip.dst==129.194.184.88



On retrouve des paquets à destination des deux adresses parce que Exch02 est, dans le cache DNS, toujours considérée comme l'adresse principale. Outlook 2013 tentera tout de même d'utiliser l'adresse principale, mais sans succès. Des paquets seront toujours transmis vers Exch02 (en moins grand nombre) mais étant donné qu'il n'y a aucune réponse, les paquets seront retransmis vers Exch01, ce qui explique la lenteur de la connexion de Outlook 2013 avec Exchange.

VI/ Conclusion

Cette partie du projet a été très intéressante car il a fallu mettre en place une architecture de serveurs multi-rôles, ce qui change légèrement la gestion des connecteurs, des ports ouverts et des flux. L'utilisation de plusieurs serveurs et les possibilités de configuration des connecteurs permettent véritablement de gérer les flux SMTP entre les rôles et les serveurs. Nous pouvons même spécifier qu'un serveur est utilisé pour la réception et un autre pour l'émission. Les possibilités sont vastes.

Il a également été possible de tester les fonctionnalités de load balancing et de failover de pfSense. On remarque que le système de loadbalancer fonctionne bien avec pfSense et Exchange 2013, mais met plus de temps à stabiliser les flux si un serveur ou service tombe en panne. D'après quelques tests de connexions SMTP et HTTPS qui ne figurent pas dans ce rapport, pfSense semble effectuer le load balancing par un mécanisme de Round Robin. La mise en place du failover s'est révélée très efficace, avec une coupure de service extrêmement courte en cas de panne d'un serveur/service.

La mise en place du cluster s'est également révélée intéressante. En effet, la détection d'un serveur en panne par le service cluster est très rapide et permet à Exchange de mettre la base de données du serveur secondaire en mode actif très rapidement.

Un aspect que Microsoft n'a pas considéré pour le moment c'est qu'une base de données Exchange qui devient active sur le serveur secondaire y reste tout le temps. et il faut une opération manuelle de l'administrateur pour l'activer à nouveau sur le serveur principal.

Lorsque tout est correctement configuré, tout le processus de failover aussi bien pour pfSense, que pour le CAS, le DAG et la base de données, est automatisé et ne nécessite aucune action supplémentaire de l'administrateur. Il est, en effet, inutile se remonter manuellement la base de données en cas de panne, tant qu'un serveur Exchange et un FSW restent en activité.

Les tests de DNS Round Robin ont été concluants. Le système fonctionne, mais il n'est pas stable. L'utilisation, le choix et le processus de « switching » des IPs est aléatoire et dépend du système d'exploitation. Une connexion fonctionnelle pour un client peut tout d'un coup devenir indisponible ou problématique à la suite d'un « switching » d'IP sur un serveur indisponible. Dans le meilleur des cas, cela ralentit la connexion. Dans le pire des cas, il y a perte de connexion. Pour maintenir une bonne disponibilité, l'administrateur doit supprimer l'entrée DNS du serveur en panne.

Par manque de temps, la dernière fonctionnalité du projet, à savoir l'utilisation d'un MX secondaire, n'a pas été testée.

V/ Annexes

5.1) Haute disponibilité

Il est important pour un système de messagerie d'être résilient. En effet, il n'est pas rare qu'un serveur tombe en panne, nécessite une maintenance, une mise à jour, une migration, etc… Dans certains cas toute coupure de service est intolérable. C'est pour cela qu'il faut intégrer au système une infrastructure redondante par le biais d'un cluster et du load balancing.

5.2) Cluster

Pour avoir un système résilient, se protéger des pannes et supporter une grande charge de travail, il y a possibilité de mettre en place un cluster. Cette fonctionnalité existe dans cette version standard de Serveur 2012, contrairement aux versions précédentes, ce qui se traduisait par des coûts supplémentaires pour se procurer la licence nécessaire. Cette fonctionnalité est obligatoire pour la haute disponibilité d'Exchange.
Un cluster est composé d'un ensemble de serveurs qui partagent des données par le biais d'un processus de réplication pour Exchange 2013. Si un des serveurs tombe en panne alors les requêtes passent par un autre serveur et on accède toujours aux mêmes données. Il n'y a pas, dans ce genre de système, de protection des données qui relève d'une autre fonctionnalité.

5.3) Load Balancing

Le load balancing est bien différent de la mise en cluster. Nous parlons ici d'une solution de haute disponibilité au niveau réseau pour le rôle CAS. Si un serveur tombe en panne, les connections sont redirigées vers les autres serveurs. Il n'y a pas de partage de données (contrairement à une mise en cluster) entre ces serveurs.

Principe de load balancing pour Exchange 2013 :

1. *A client resolves the namespace to a load balanced virtual IP address*
2. *The load balancer assigns the session to a CAS member in the load balanced pool*
3. *CAS authenticates the request and performs a service discovery by accessing Active Directory to retrieve the following information*
    - *Mailbox Version*
    - *Mailbox Location*
4. *CAS makes a decision on whether to proxy the request or redirect the request to another CAS infrastructure (within the same forest)*
5. *CAS queries an Active Manager instance that is responsible for the database to determine which Mailbox server is hosting the active copy*
6. *CAS proxies the request to the Mailbox server hosting the active copy*[13]

[13] http://blogs.technet.com/b/exchange/archive/2014/03/05/load-balancing-in-exchange-2013.aspx

7. Nous avons ici la possibilité de mettre en place un load balancing de couche 4 (ne prenant en compte que l'IP et le port). Effectivement, grâce à Exchange 2013, nous n'avons plus besoin d'avoir l'affinité de session (processus par lequel une fois qu'une connexion était créée entre le client et le CAS, elle devait rester sur ce CAS).

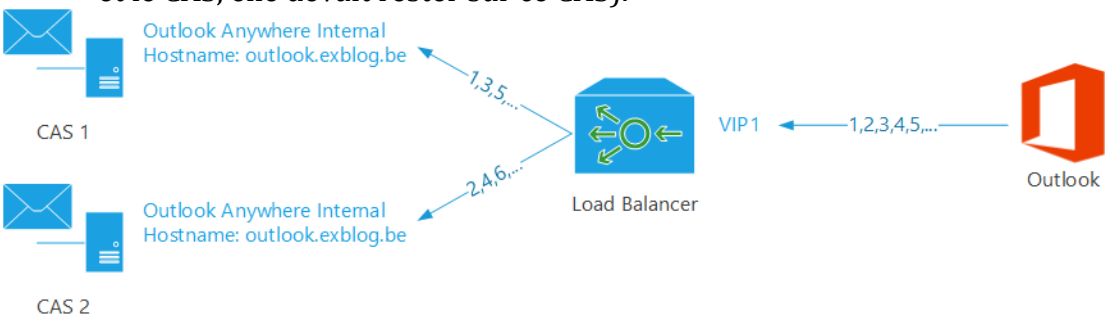


Figure 27 : Load Balancing[14]

Le load balancer est donc chargé de rediriger les requêtes des clients vers les différents CAS en fonction du trafic. Les CAS doivent partager les mêmes FQDN publics. En cas de panne, la redirection est automatique et transparente pour l'utilisateur (pas d'affinité de session).

- Haute disponibilité plus facile à mettre en place
- Load Balancing de couche 4 (CAS avec connexion stateless. Pas d'affinité de session pour le load balancer. Un utilisateur n'est pas lié à un CAS ou MBX seul)

5.4) Echanges avec le FSW

Voici une capture d'écran Wireshark montrant l'échange de données avec le FSW et les serveurs Exchange. L'échange de données se fait par le protocole SMB2 entre le FSW et un seul serveur Exchange. Si Exch01 tombe en panne, alors Exch02 communiquera avec le FSW. Il n'y a pas eu assez de temps à disposition pour étudier le contenu des échanges. Les fichiers dans le dossier du FSW ne contiennent aucune information compréhensible ou lisible.

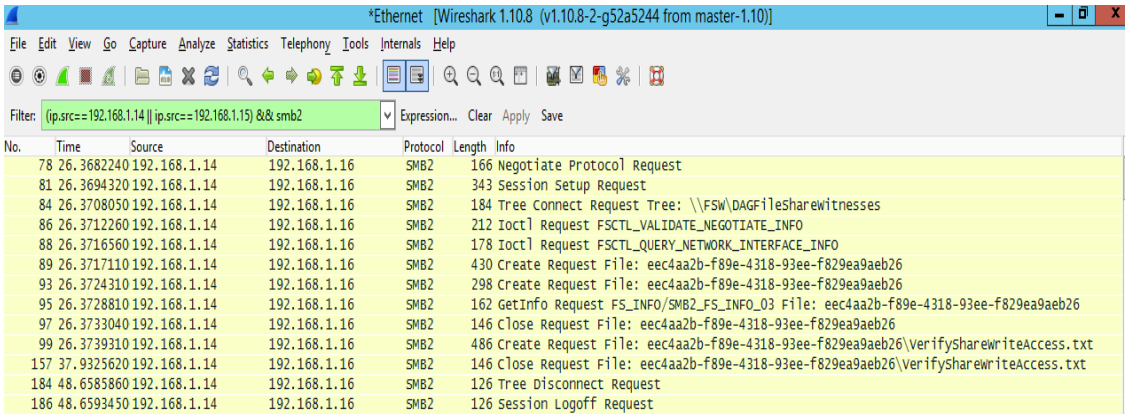


Figure 28 : Echanges FSW

[14]http://d236s0uss5g0vh.cloudfront.net/files/reviewes/MS%20Exchange%202013:%20Useful%20blog%20post%20about%20load%20balancing%202013%20vs%202010/image9.png