La configuration d'Outlook Anywhere sur Exchange 2013

http://itnyou.fr/outlookanywhere2013/

Introduction

Description rapide :

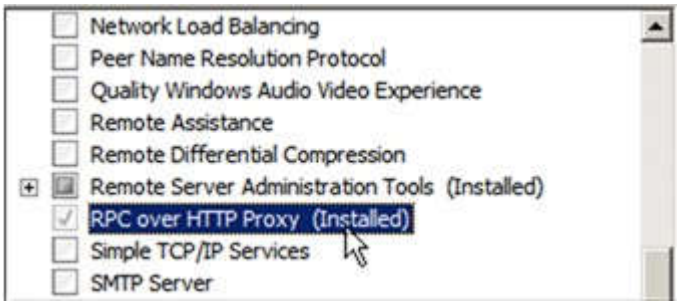
Outlook Anywhere permet aux clients qui utilisent Outlook 2013, Outlook 2010, Outlook 2007 d'accéder à (sa/ses) boites aux lettres Exchange directement depuis Internet sans VPN.

Dans les versions précédentes d'Exchange (2003/2007/2010), il était nécessaire d'activer manuellement Outlook Anywhere et de le configurer.

Avec Exchange 2013, Outlook Anywhere est activé par défaut car le MAPI /RPC n'est plus utilisé, toute la connectivité Outlook s'effectue en rpc over http(S). En l'occurrence, il n'est donc plus nécessaire d'utiliser des ports statiques RPC ou des grandes de plages de ports pour le load balancing.

Prérequis :

- Vu qu'Outlook anywhere est activé par défaut sur Exchange 2013, le composant Windows Proxy RPC sur http doit être installé à l'installation du serveur CAS.
  Si vous n'avez pas installé le composant à l'installation du serveur CAS, vous pouvez le faire maintenant soit via le gestionnaire de serveur en y ajoutant une fonctionnalité :



Ou à l'aide de la ligne de commande suivante :

ServerManagerCmd -i RPC-over-HTTP-proxy

- Un certificat SSL valide mais vous pouvez utiliser les mêmes url et le même certificat que pour outlook Web access et Activesync ou alors utiliser un certificat auto-signé avec les SAN adéquates (nom des serveurs CAS, nom du casarray, url externe, url interne …)

- Avoir les entrées DNS interne et externe nécessa
- ires (nom des serveurs CAS, nom du casarray, url externe, url interne …)

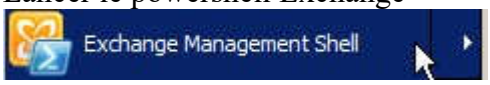
Voici la Technet Microsoft pour Outlook anywhere 2013 :
http://technet.microsoft.com/fr-fr/library/bb123741(v=exchg.150).aspx

Configuration d'Outlook Anywhere 2013

Une fois que vous avez tous les prérequis, vous pouvez maintenant configurer Outlook Anywhere. Vous pouvez effectuer ceci soit avec la console web Exchange Admin Center (EAC) disponible via l ECP ou soit avec le powershell Exchange, qui à mon avis plus rapide, mais biensur aussi moins conviviale qu'une interface GUIJ.

Pour faire la configuration via powershell :

Lancer le powershell Exchange



Utiliser la commande Set-Outlook Anywhere
Exemple:

Set-OutlookAnywhere –Server SVSTD-EXC01 –ExternalHostname webmail.mondomaine.com –InternalHostname svstd-exc01.mail.dom –ExternalClientAuthenticationMethod Ntlm –InternalClientAuthenticationMethod Ntlm –IISAuthentication Ntlm –SSLOffloading:$false

Voici le résultat:

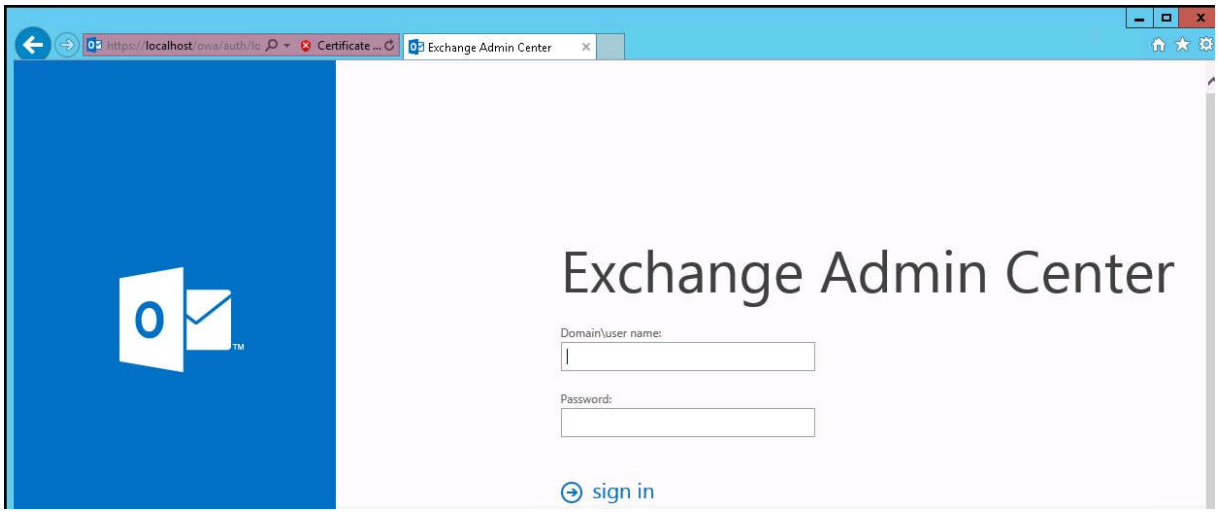
Get-OutlookAnywhere –Server SVSTD-EXC01

```
ServerName                      : SVSTD-EXC01
SSLOffloading                   : False
ExternalHostname                : [redacted]
InternalHostname                : svstd-exc01.mail.dom
ExternalClientAuthenticationMethod : Ntlm
InternalClientAuthenticationMethod : Ntlm
IISAuthenticationMethods        : {Ntlm}
XropUrl                         :
ExternalClientsRequireSsl       : True
InternalClientsRequireSsl       : True
MetabasePath                    : IIS://SVSTD-EXC01.mail.dom/W3SVC/1/ROOT/Rpc
Path                            : C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\rpc
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags         : {}
ExtendedProtectionSPNList       : {}
AdminDisplayVersion             : Version 15.0 (Build 712.24)
Server                          : SVSTD-EXC01
```

Pour faire la configuration via la console web Exchange Admin Center :

Via votre navigateur web sur le serveur CAS, aller à l'url : https://localhost/ecp
Accepter et ignorer ainsi l'avertissement de sécurité du certificat.

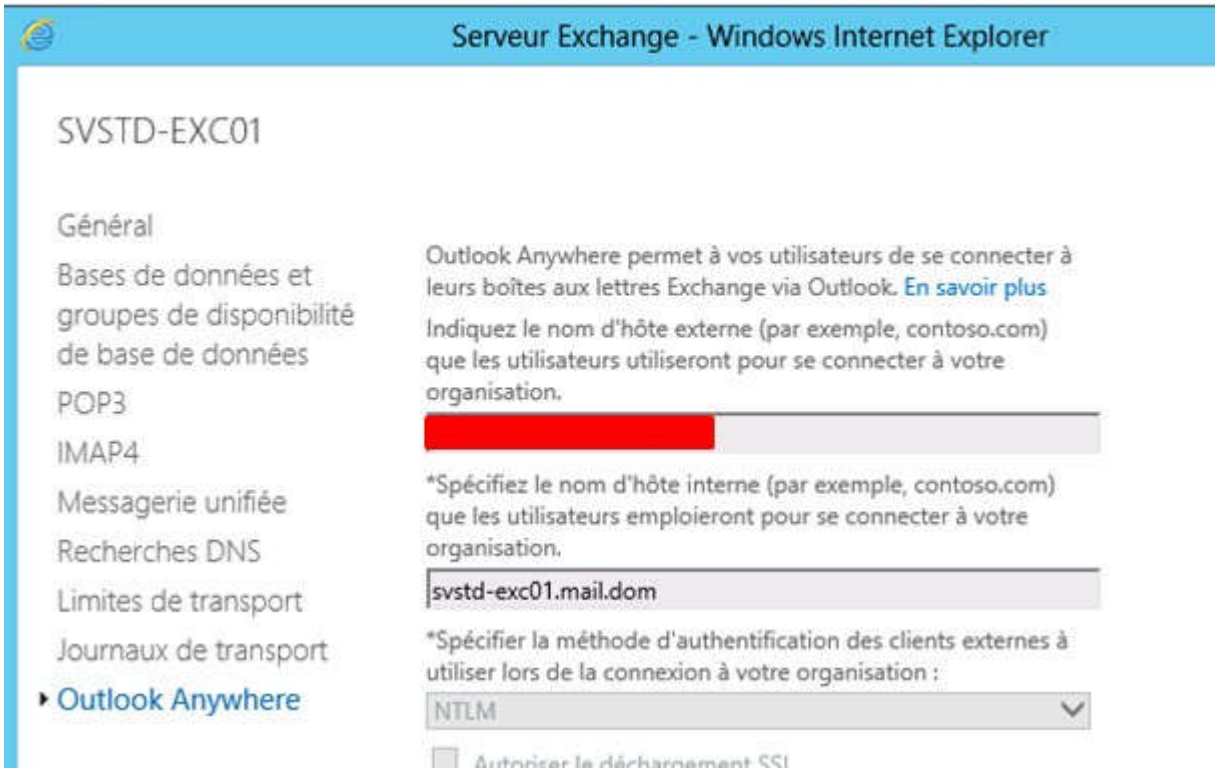
La page Exchange Admin Center apparait alors, identifiez vous avec un ou votre compte d'administration Exchange.



Une fois loggué dans l'Exchange Admin Center, cliquez sur Serveurs sur la partie gauche :

Dans le menu Serveurs, double cliquez sur le serveur que vous souhaitez configurer

Sélectionnez ensuite « Outlook Anywhere », vous pouvez maintenant configurer les urls internes et externes ainsi que le type d'authentification que vous souhaitez utiliser pour Outlook Anywhere



Une fois les champs complétés, cliquez sur « Enregistrer » pour sauvegarder et appliquer vos paramètres.

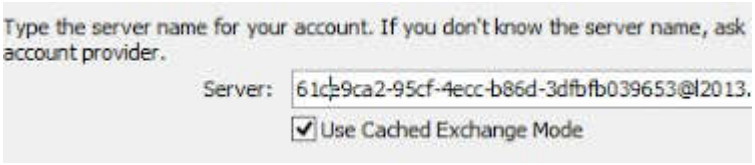
Vous avez maintenant configuré Outlook Anywhere 2013.
Vous ne pourrez biensur le tester en externe qu'une fois la publication via reverse proxy (TMG/ISA ou autres) effectuée.
(Prochain article sur Exchange 2013 & publication TMG)

Informations supplémentaires :

- Si vous souhaitez blocker Outlook Anywhere rpc/http pour un ou un panel d'utilisateur, vous pouvez utiliser l'attribut « MAPIBlockOutlookRpcHttp »
  Exemple :
  Pour un utilisateur spécifique :
  Get-Mailbox –Identity <user> | Set-CASMailbox -MAPIBlockOutlookRpcHttp:$True
  Pour tous les utilisateurs :
  Get-Mailbox –ResultSize Unlimited | Set-CASMailbox -MAPIBlockOutlookRpcHttp:$True

- Les clients Outlook ne se connectent plus avec le fqdn du serveur ou de votre casarray comme dans les versions précédentes d'Exchange.
  Les clients Outlook utilisent l'autodiscover pour se connecter à Exchange 2013 avec le guid de la boite aux lettres de l'utilisateur.
  Ceci à priori pour quasiment supprimer le message : « Votre administrateur a apporté des

modifications à votre boîte aux lettres. Veuillez redémarrer votre client Outlook»
Exemple :



http://msexchangeguru.com/2013/01/10/e2013-outlook-anywhere/

Exchange 2013: Configuring Outlook anywhere

In Exchange 2013, Outlook Anywhere is enabled by default, because all Outlook connectivity takes place via Outlook Anywhere anyways.

Thats' right. Its all HTTP now from exchange 2013. The Windows RPC over HTTP Proxy component, which Outlook Anywhere clients use to connect, wraps remote procedure calls (RPCs) with an HTTP layer. This allows traffic to traverse network firewalls without requiring RPC ports to be opened.

Follow the steps to configure Outlook anywhere in Exchange 2013 server.

1. From EAC, click Servers as shown and double click on the server name.

https://www.sylvaincoudeville.fr/2015/04/les-bases-dune-bonne-configuration-exchange-partie-4/

Activation OutlookAnywhere

A quoi ça sert?

OutlookAnywhere est un protocole permettant à un Outlook qui est habituellement connecté au LAN privé, et qui utilise Active Directory, de pouvoir se synchroniser aussi à l'extérieur de l'entreprise.

C'est cette fonctionnalité qui doit être activée pour que des postes hors domaine puissent utiliser Outlook de manière correcte.

Configuration pour Exchange 2010

Pour activer OA (OutlookAnywhere), ouvrez un EMS (Exchange Management Shell) :

```
Enable-OutlookAnywhere -Server 'EXCH2013' -ExternalHostname
'mailhost.sylvaincoudeville.fr' -DefaultAuthenticationMethod 'Basic' -
SSLOffloading $false
```

Maintenant, il faut patienter 15 minutes afin que la fonctionnalité s'active.

Configuration pour Exchange 2013

Pour configurer OA (OutlookAnywhere), ouvrez un EMS (Exchange Management Shell) :

```
Get-OutlookAnywhere|Set-OutlookAnywhere -ExternalHostname
'mailhost.sylvaincoudeville.fr' -InternalHostname
'mailhost.sylvaincoudeville.fr' -ExternalClientsRequireSsl $true -
InternalClientsRequireSsl $false
```

On peut améliorer la sécurité en passant le paramètre 'InternalClientsRequireSsl' à $true.

Maintenant, il faut patienter 15 minutes afin que la fonctionnalité s'active.

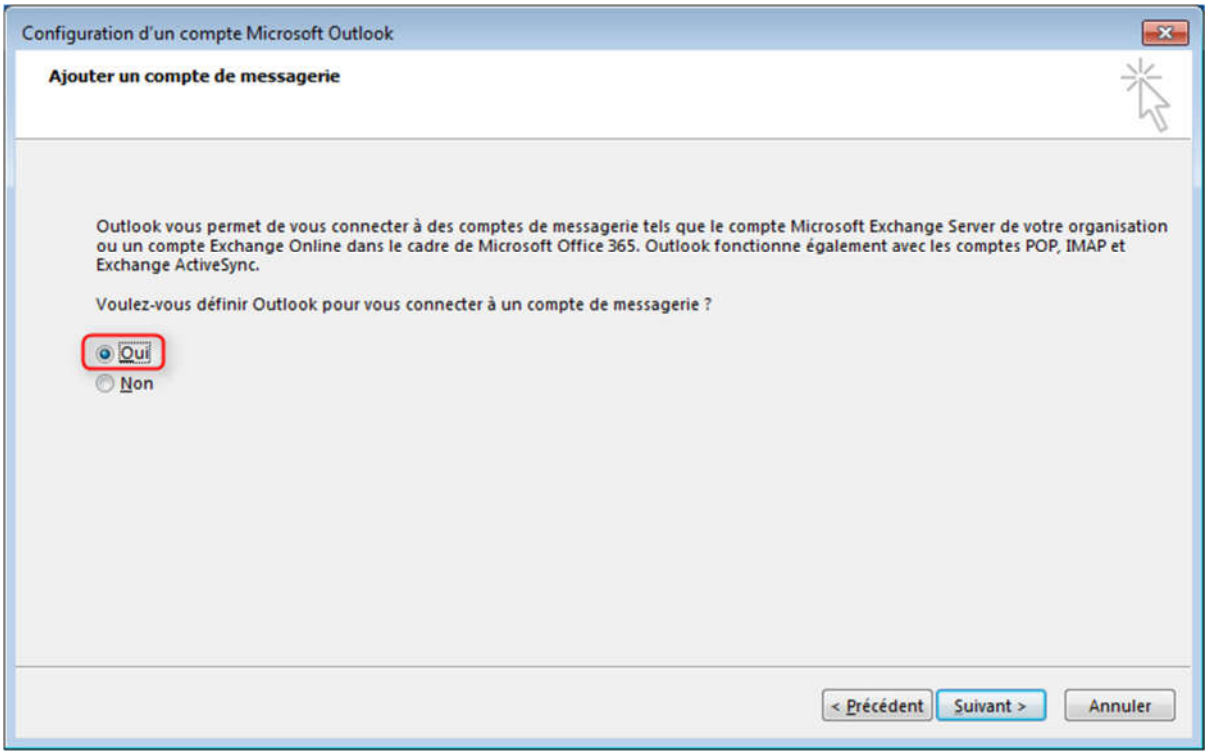
Configuration Outlook

Nous allons voir ici la configuration d'Outlook hors et dans un domaine.

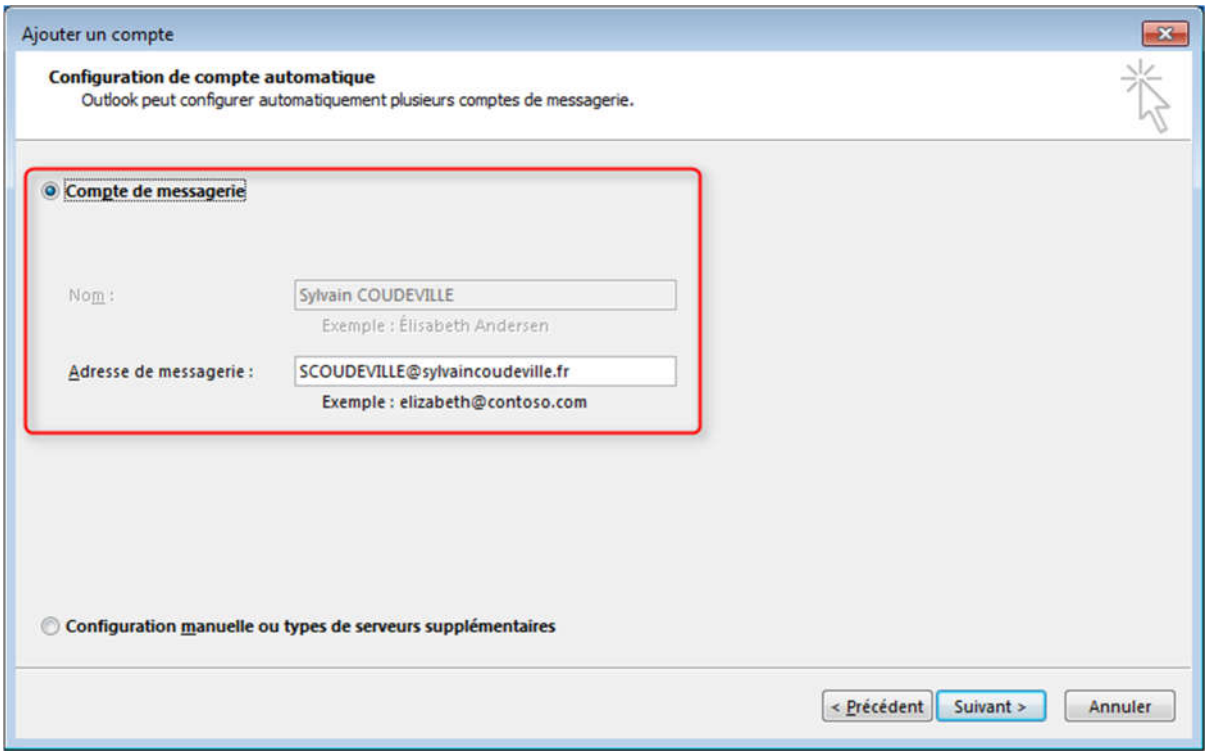
Vous verrez que la jonction au domaine est vraiment un énorme plus. Alors, par pitié, arrêtez de travailler hors domaine !

Outlook dans le domaine

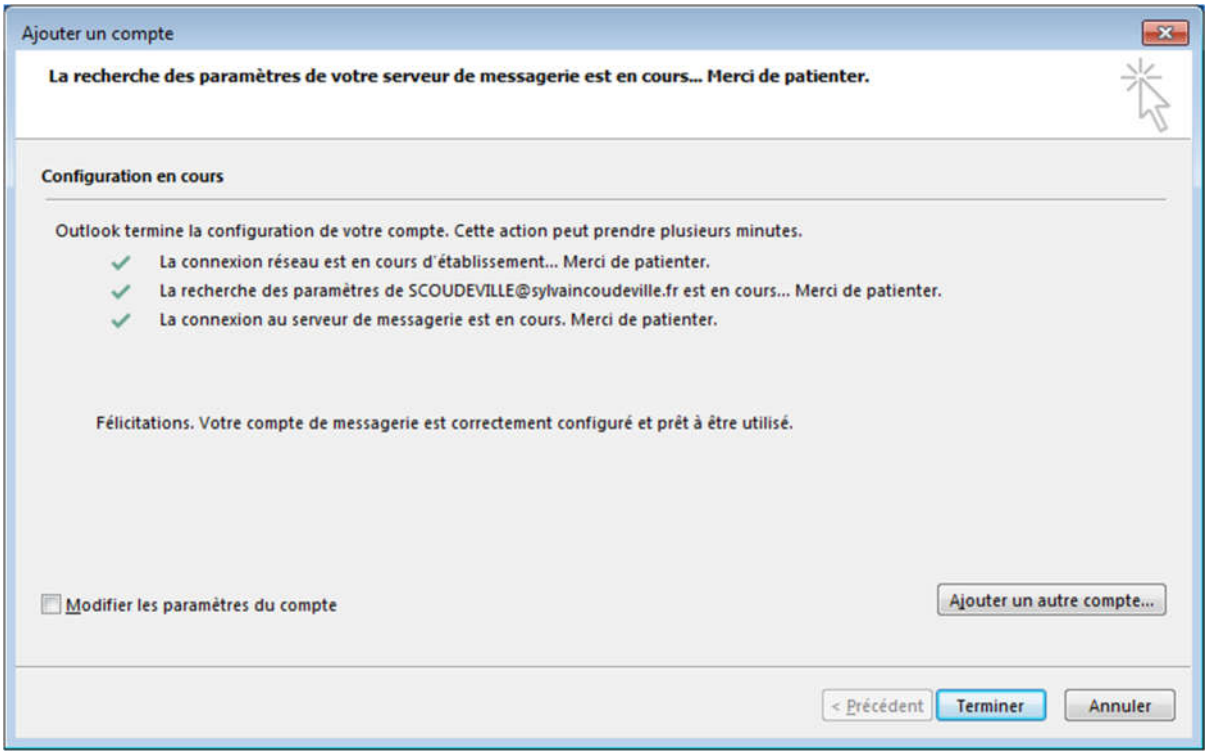
Prenons une machine jointe au domaine monAD.local, et logguée sur le domaine (utilisateur MONAD\s.coudeville, dans notre exemple) et lançons Outlook:



On configure… rien, tout s'est saisi seul :



Et à l'étape suivante, tout se valide sans erreur (car nous avons tous bien travaillé!) :



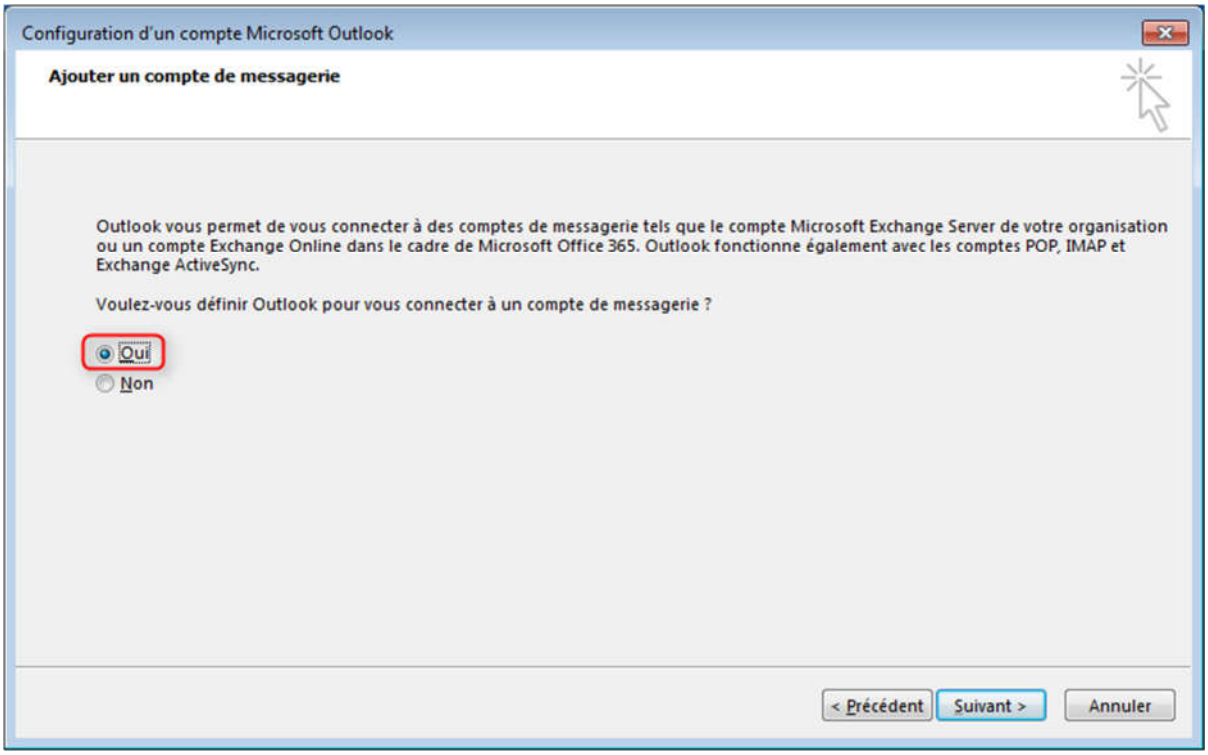
Et c'est terminé !

Tout va se connecter, pas de prompt du nom d'utilisateur/mot de passe, pas d'erreur de certificat !

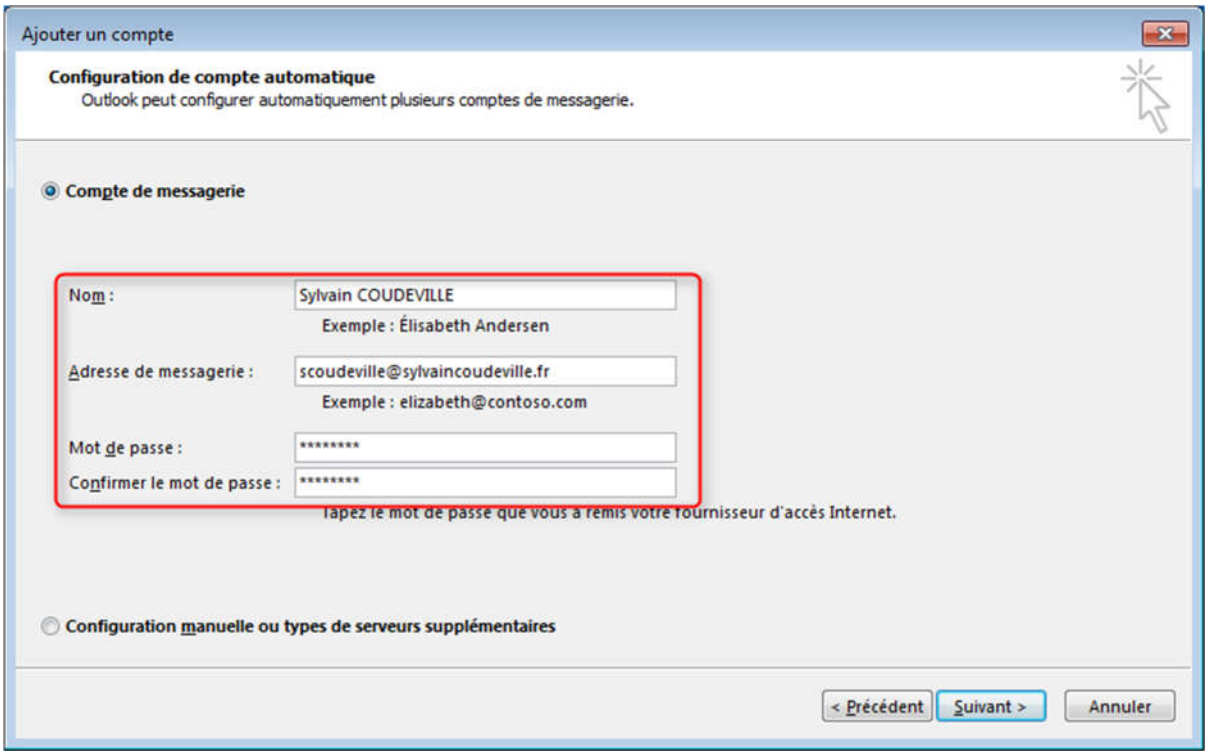
Essayez maintenant d'utiliser cette machine et cette session en dehors du LAN de l'entreprise : cela fonctionnera aussi !

Outlook hors domaine

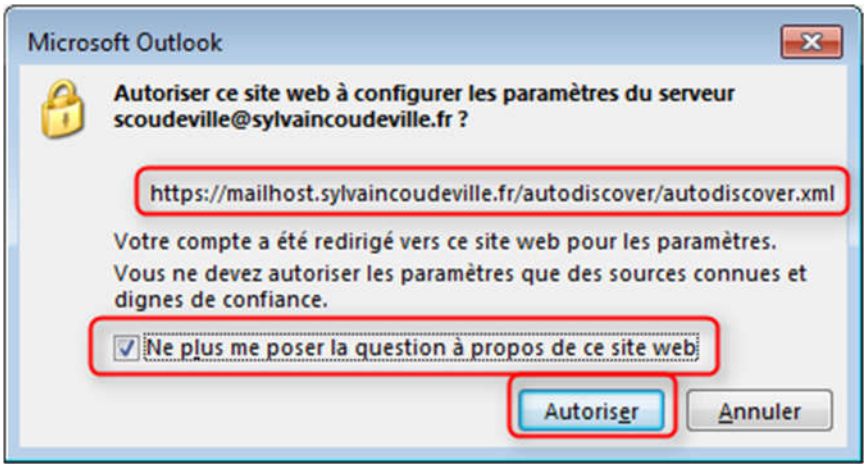
Maintenant, nous allons prendre une autre machine, hors domaine avec un compte local et lancer Outlook :



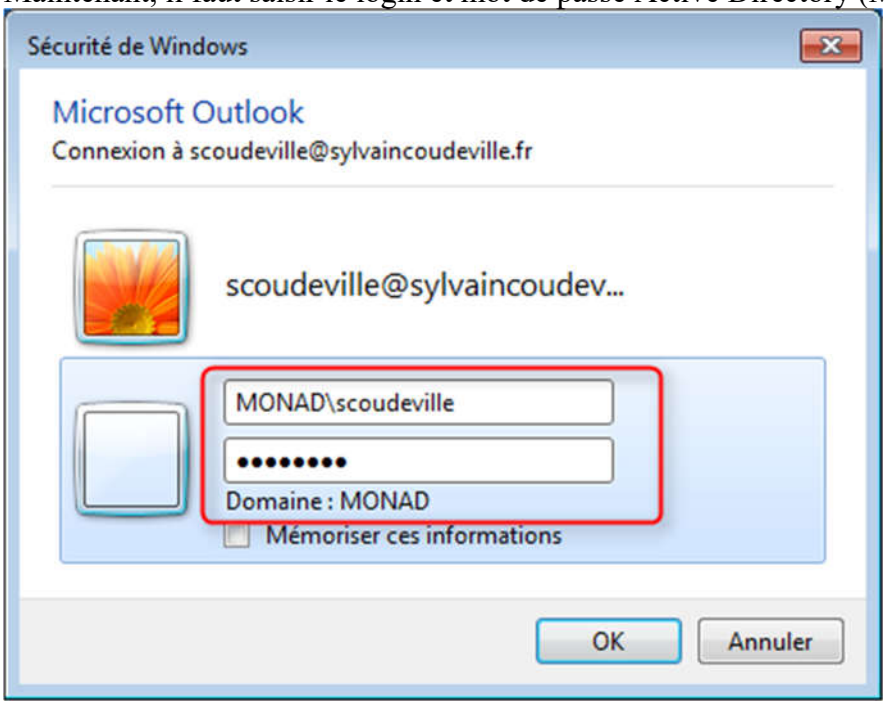
Et maintenant, on saisit adresse email, et mot de passe :



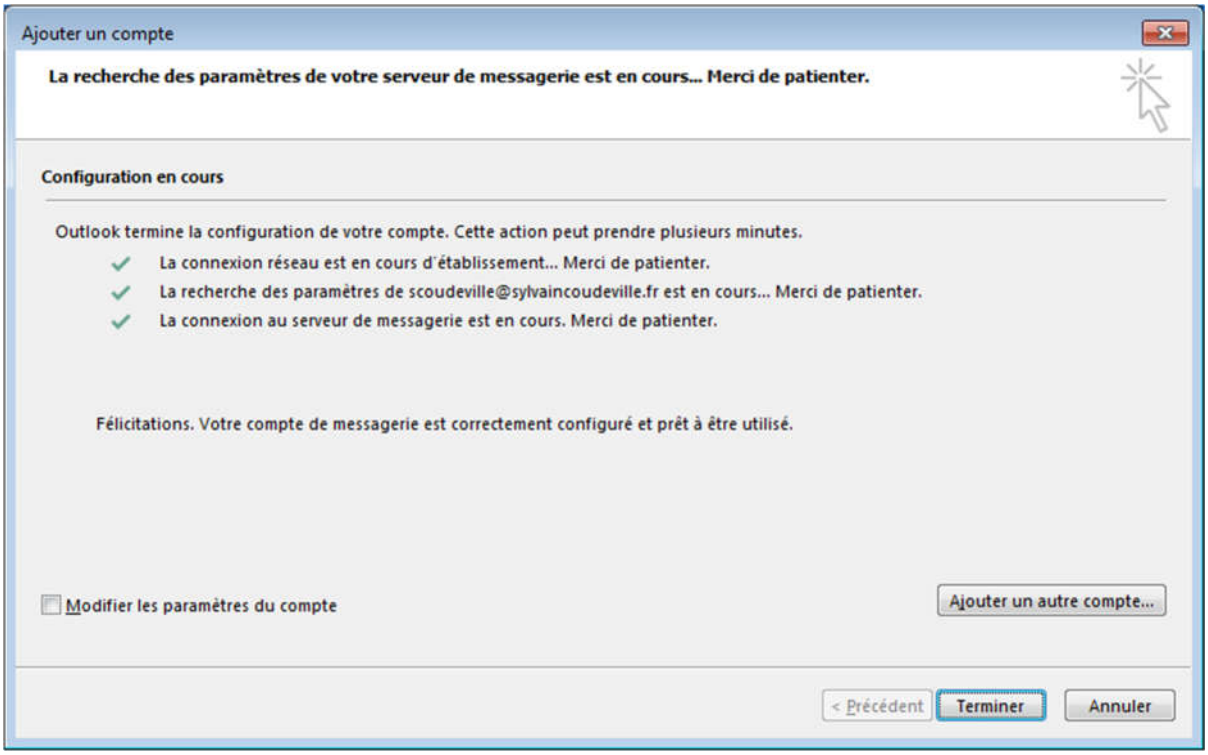
Grâce au DNS bien configuré (enregistrement SRV), Outlook trouve le service Autodiscover au bon endroit :



Maintenant, il faut saisir le login et mot de passe Active Directory (MONAD\scoudeville) :

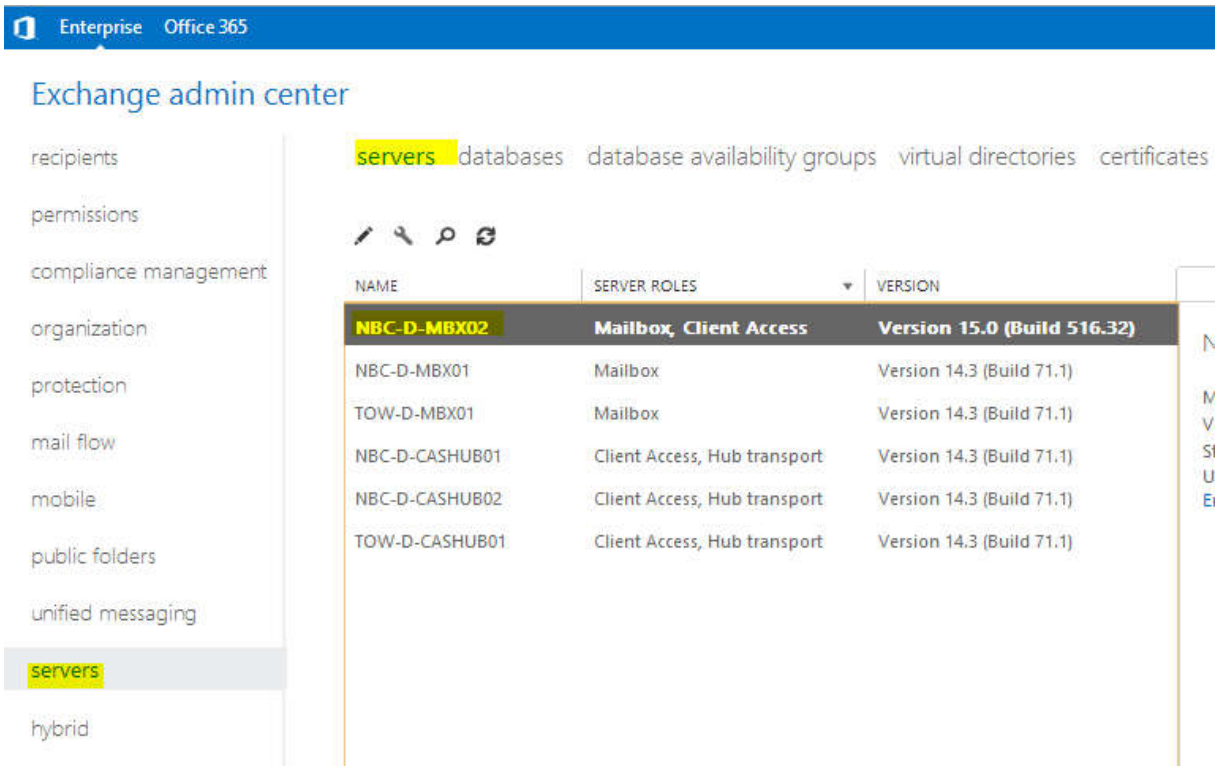


Il faudra peut-être ressaisir les informations plusieurs fois. Si tout est OK, la configuration devrait se terminer sans erreur :



Et c'est terminé.

Par contre, l'utilisateur se verra demander son login et mot de passe de domaine à chaque ouverture d'Outlook (si vous ne le stockez pas).

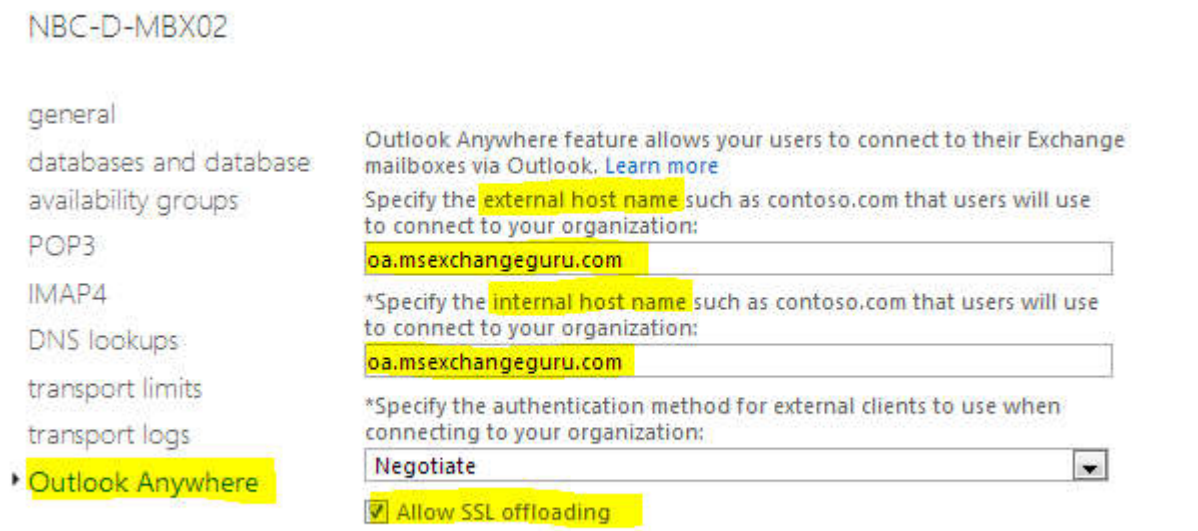


2. Before you proceed please ensure that you have configured a certificate to use with Outlook Anywhere. You may leave the external hostname blank if you do not want your external clients to connect to Outlook Anywhere from internet.

If you wish to **disable Outlook anywhere over the internet in Exchange 2013, simply leave the external hostname entry blank !!! This will ensure that only internal users can access Outlook…**

Outlook Anywhere for a user depends on the attribute “MAPIBlockOutlookRpcHttp” which can be found by running the cmdlet:

Get-CASMailbox alias | Name, *MAPIBlock*



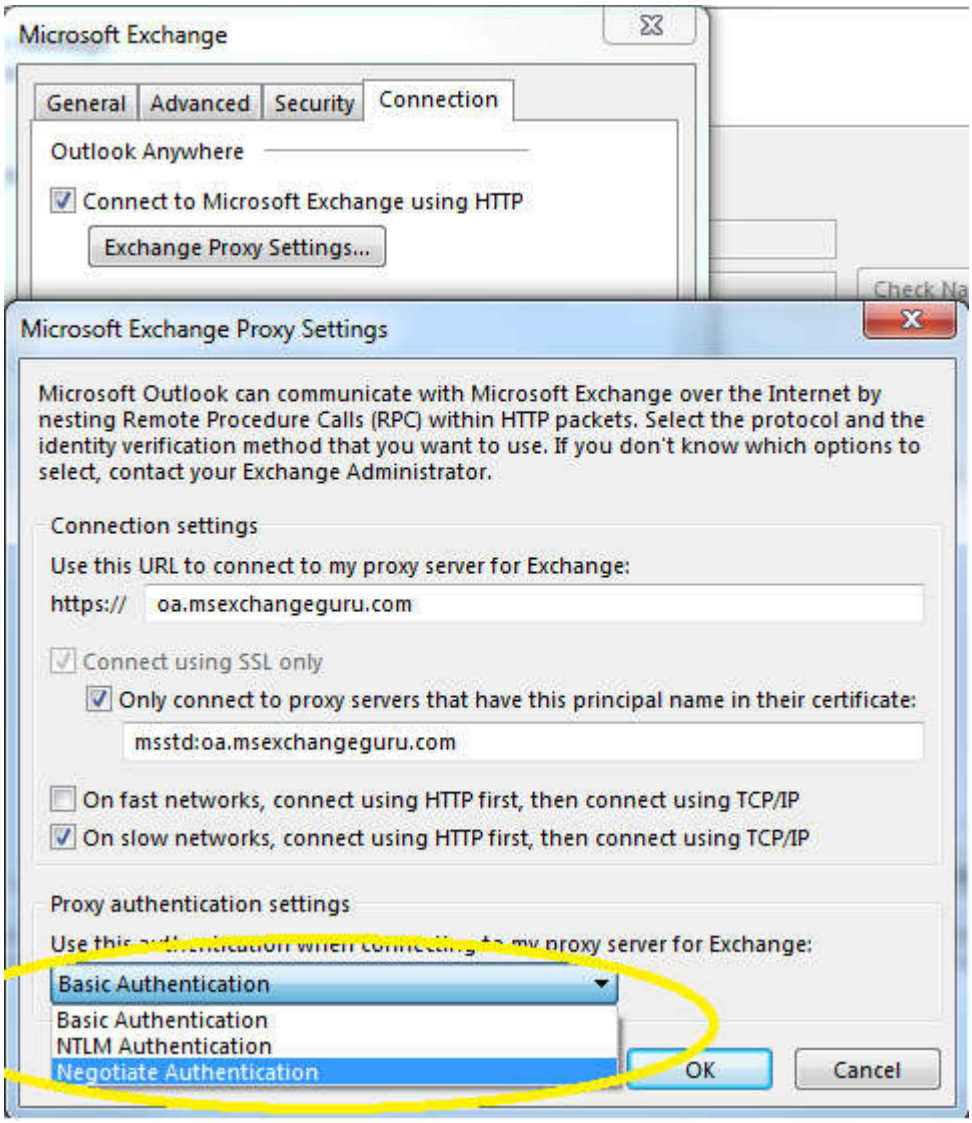
It is important for you to understand the difference between several authentication types Exchange offers for Outlook Anywhere

Basic authentication: If you select this authentication type, Outlook will prompt for username and password while attempting a connection with Exchange.

NTLM authentication: If you select this authentication type, exchange does not prompt users for a user name and password. The current Windows user information on the client computer is supplied by the browser through a cryptographic exchange involving hashing with the Web server. If the authentication exchange initially fails to identify the user, the browser will prompt the user for a Windows user account user name and password. So, when Outlook is trying to connect to Exchange and if the machine is domain joined, there isn't a need to provide password.

Negotiate authentication: Enabled by default in Exchange 2013. This is a combination of Windows integrated authentication and Kerberos authentication. If we employ negotiate authentication, exchange will authenticate the client using NTLM authentication type and if unable to verify authenticity, will challenge the client to authenticate using a username and password.

If you look at Outlook settings –> Account Settings –> More Settings –> Connection, you may see the same authentication settings.



When we configure Outlook Anywhere and select an authentication type, Autodiscover will update outlook client with all URL details and authentication type.

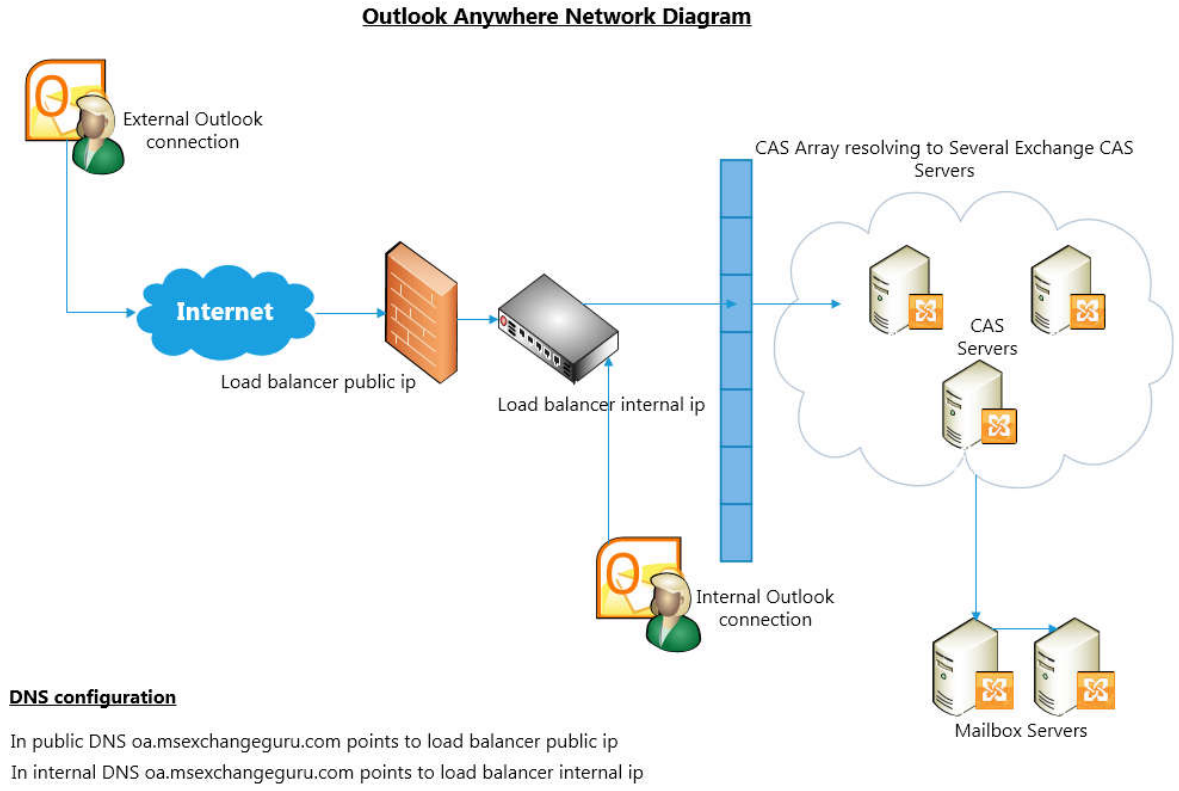
Always note that you should not be mislead with proxy settings in Outlook alone. If you have a different URL configured for InternalHostname and ExternalHostName, Outlook proxy settings will only show InternalHostname and this is by design.

Outlook Exchange Proxy Settings dialog box always displays the internal host name as the Proxy server in an Exchange Server 2013 environment:
http://support.microsoft.com/kb/2754898

Configuring high availability for Outlook anywhere in Exchange 2013:

In my case, I have the following configuration for load balancing and redundancy:

URL oa.msexchangeguru.com will have 2 interface on a hardware load balancer as shown:



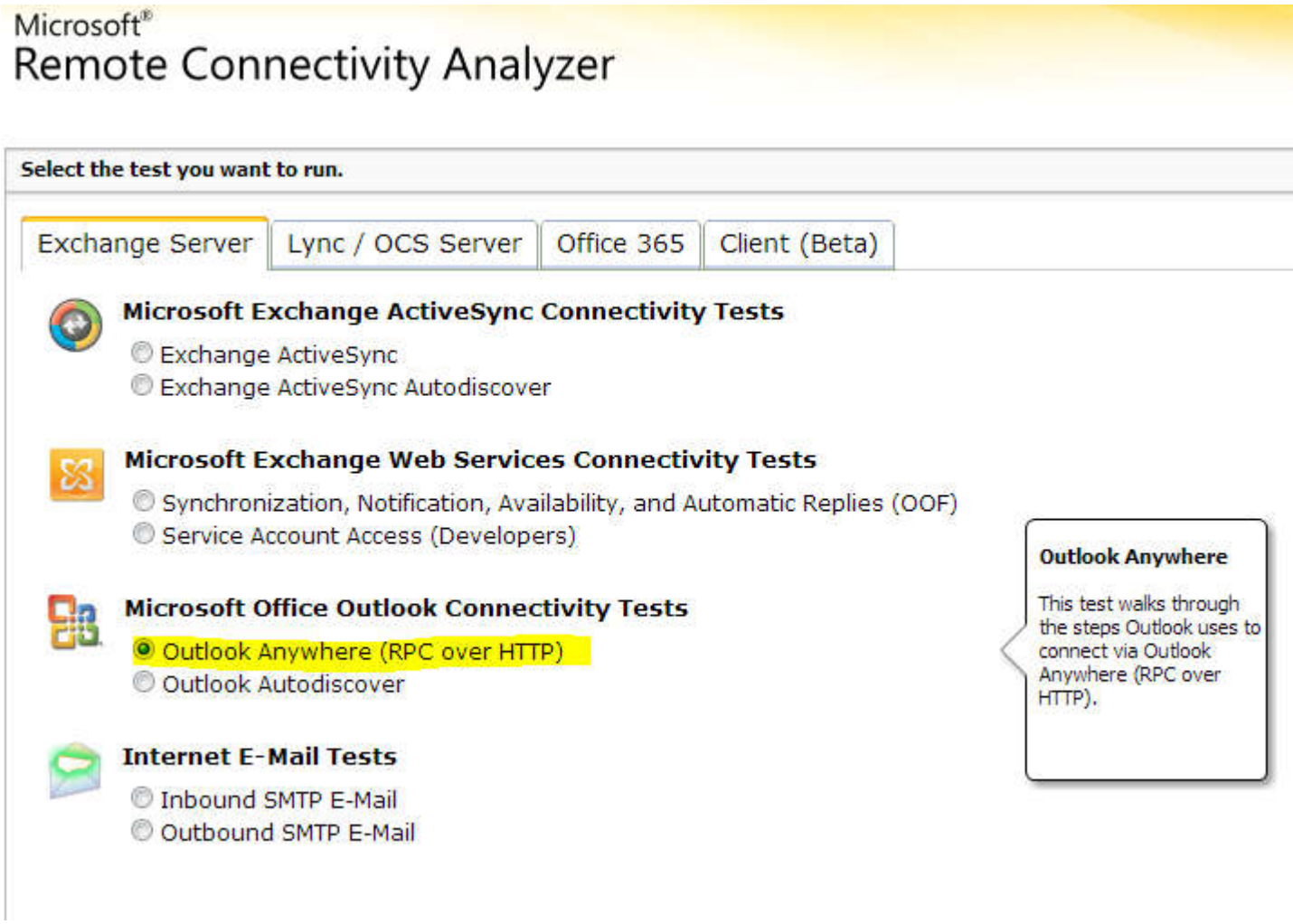
Any client which tries to establish a connection from internet will talk to the external DNS record for the OA URL pointing to a firewall which inturn points to the load balancer.

All internal clients are pointed to the load balancer internal ip to bypass the firewall.

Testing Outlook Anywhere in exchange 2013:

Testexchangeconnectivity.com or Exchange Remote Connectivity Analyzer (ExRCA) is an service offered by Microsoft in their inhouse data center which enables companies to test their Exchange features over the internet.

Navigate to testexchangeconnectivity.com and select the following option:



You may also use **Test-OutlookConnectivity.** The cmdlet tests for Outlook Anywhere (RPC over HTTP) connections. If the cmdlet test fails, the output notes the step that failed.