Le Serveur de Communication IceWarp

Guide de sécurité

Version 12

Mars 2018

Sommaire

Guide de sécurité 2

Guide de sécurité

Introduction

L'objectif de ce document est de présenter les règles de sécurité qui peuvent être mises en œuvre sur le serveur IceWarp. Les règles de sécurité ont pour objectif de protéger le serveur vis à vis du réseau (confidentialité, déni de service, blacklistage par les autres serveurs...) et de protéger les utilisateurs (confidentialité, virus, Spams...).

Il donne des règles et des conseils de mise en œuvre, il est destiné à l'administrateur du serveur pour qu'il configure son serveur et qu'il donne aux utilisateurs les directives de configuration de leur client de messagerie.

Nous ne traitons ici que de la messagerie asynchrone (protocoles SMTP, POP et IMAP) par opposition à la messagerie instantanée.

Les mécanismes Anti-Virus et Anti-Spam font aussi partie de la sécurité du serveur mais sont traités dans des documents spécifiques.

Des documents complémentaires sont téléchargeables sur

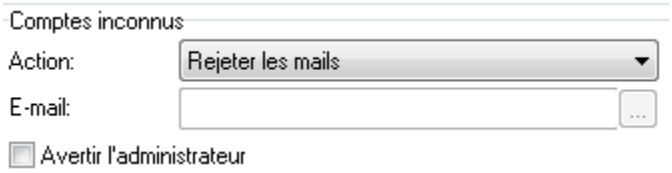
- Le site www.icewarp.fr (télécharger -> Documentation).
- Le site support.icewarp.fr (base de connaissances en particulier)

La sécurité vue du serveur

La sécurité au niveau des domaines

Destinataires inconnus

Dans le menu Gestion -> Domaines et Comptes -> <domaine> -> onglet Options il y a la fenêtre suivante :



Qui permet de traiter les comptes qui ne sont pas connus du domaine.

- "Rejeter les mails" est le meilleur.
- "Catch all" est dangereux en cas d'attaque par des alias aléatoires.
- "Supprimer" ne permet pas à l'expéditeur de savoir que son message n'a pas été reçu.

Limitation des envois

La limitation du nombre d'envois effectué par chaque utilisateur peut avoir des raisons contractuelles mais c'est aussi une façon de se protéger contre le relayage involontaire si un mot de passe a été trouvé par un spammeur.

Les limites peuvent être placées :

- Au niveau du domaine, onglet "Limites" du domaine dans le groupe "Domaine" : "Nombre maximum d'envois par jour". Cette limite est prédominante sur les autres limites.

- Au niveau des utilisateurs pour tout le domaine, onglet "Limites" du domaine dans le groupe "Utilisateurs" : "Nombre maximum d'envois par jour"

- Au niveau de chaque utilisateur : onglet "Limites" du compte : "Nombre maximum d'envois (/jour)". Cette limite est prédominante sur la limite utilisateur définie au niveau du domaine.

La valeur 0 indique qu'il n'y a pas de limite.

Ces limites ne s'appliquent qu'aux emails envoyés vers l'extérieur mais seules les "Client session" sont comptabilisées.

Cela signifie que si un message contient plusieurs destinataires du même domaine, ils ne seront comptés qu'une seule fois.

Le compteur qui comptabilise ce nombre est accessible par la console d'administration dans Etat -> Statistiques comptes -> onglet Liste -> "# envoyés extérieur".

Les envois à une liste de diffusion ne sont pas comptabilisés, il est donc important de sécuriser les listes (Voir la FAQ).

Il peut être aussi intéressant de limiter le nombre de destinataires par email dans Email -> Général -> Avancé -> "Nb. max de destinataires pour un email entrant" dont la valeur par défaut est 32768.

Il s'agit de contrôler le nombre de commandes 'RCPT TO:' autorisées dans une session serveur SMTP. Ce réglage s'applique à tout le serveur (tous les domaines et tous les comptes)

La sécurité du service de messagerie

Ces options permettent de se protéger contre l'utilisation intempestive du serveur par des utilisateurs mal intentionnés et contre des attaques de type "déni de service" qui visent à rendre le serveur inopérant en le saturant de fausses demandes.

Remarque : Le relayage consiste à recevoir un message de l'extérieur (par SMTP ou POP) et à le retransmettre vers un serveur distant (c'est à dire que le destinataire n'est pas local).

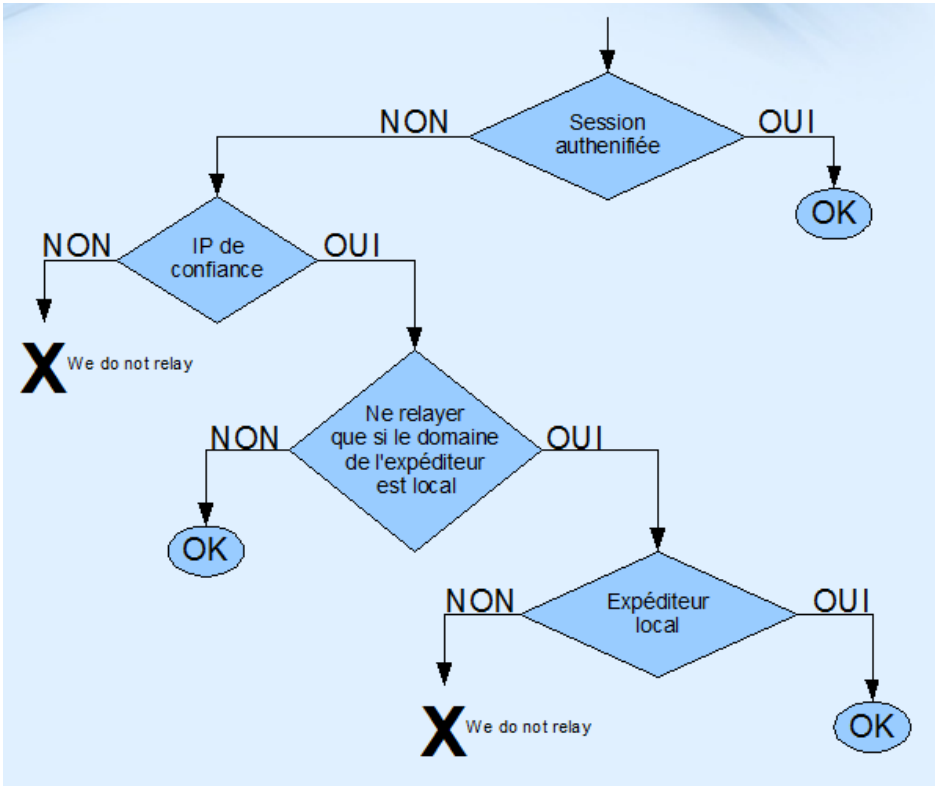
L'anti relayage : des spammeurs (ou autres...) cherchent à utiliser le serveur comme relais pour envoyer leurs mails ce qui peut avoir comme conséquence de faire passer votre serveur pour un émetteur de Spams et peut conduire à le faire mettre en liste noire. Le moyen le plus sûr pour éviter le relayage intempestif est de n'accepter que les expéditeurs authentifiés.

Le contrôle de l'expéditeur : ceci s'effectue en contrôlant l'adresse IP de l'expéditeur et son nom de domaine (listes noires, rDNS, SPF...).

La prévention des intrusions : les tentatives provenant d'une adresse IP peuvent être limitées de façon à rejeter au plus vite les connexions dont on pense qu'elles sont abusives.

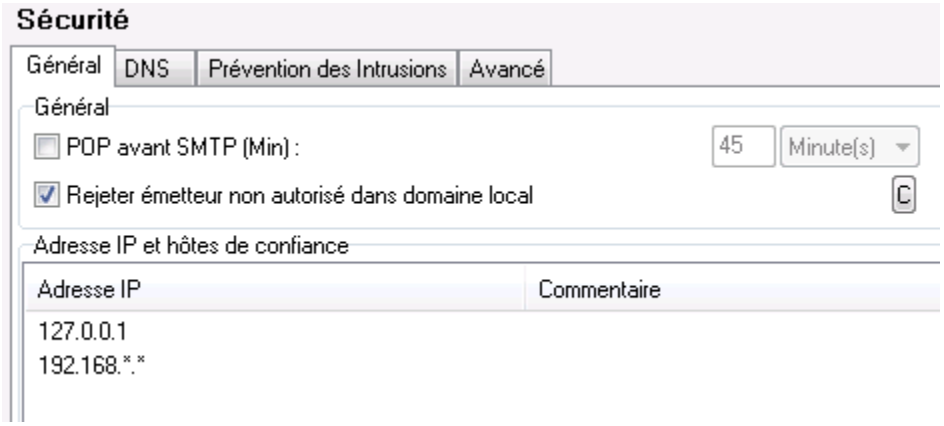
Il faut noter que la principale protection du serveur repose sur le couple **utilisateur/mot de passe**. Il est donc extrêmement important que ces informations soient confidentielles et impossible à deviner (rejeter les couples trop standards de type admin/admin ou administrateur/password...). La stratégie des mots de passe aide à définir des mots de passe difficiles à casser.

Le schéma ci-dessous résume les cas où le relayage est autorisé et les cas où il ne l'est pas :



Paramètres généraux

Ces paramètres sont accessibles dans le menu Email -> Sécurité -> onglet Général :



Pour la sécurité, le relayage est implicitement contrôlé, ceci oblige l'émetteur à se faire accepter par au moins une des méthodes suivantes :

- **Authentification** de l'échange SMTP par un couple nom d'utilisateur/mot de passe. Il suffit de donner les références du compte POP si les serveurs POP et SMTP sont identiques, sinon, il faut donner les références du compte SMTP (dans le client).
- **POP authentifié** moins de n minutes avant l'envoi SMTP (ce mécanisme marche si le serveur SMTP est le même que le serveur POP/IMAP). Il faut que l'option "**POP avant SMTP (Min)**" soit cochée dans l'écran ci-dessus. C'est une méthode **dangereuse** car elle ouvre une porte de relayage sur la machine de l'émetteur pendant un temps important.
- Faire partie des **émetteurs de confiance** qui sont listés dans la fenêtre "Adresse IP et hôtes de confiance". On peut y placer les clients du réseau local (par ex : 192.168.*.*).

Le non respect de l'authentification se traduit dans le journal SMTP par un message d'erreur du type:

550 5.7.1 <user1@domaine1>... we do not relay <user2@domaine2>

L'option "**Rejeter l'émetteur non autorisé dans domaine local**" impose à tout compte reconnu comme local (l'adresse mail utilise un domaine local) de s'identifier même si le destinataire est local. Cette option est **fortement conseillée**, elle assure que tous les utilisateurs locaux utilisent l'authentification SMTP. Le non respect de cette règle provoque l'erreur :

550 5.7.1 <user1@domaine1> Access to < user2@domaine2> not allowed

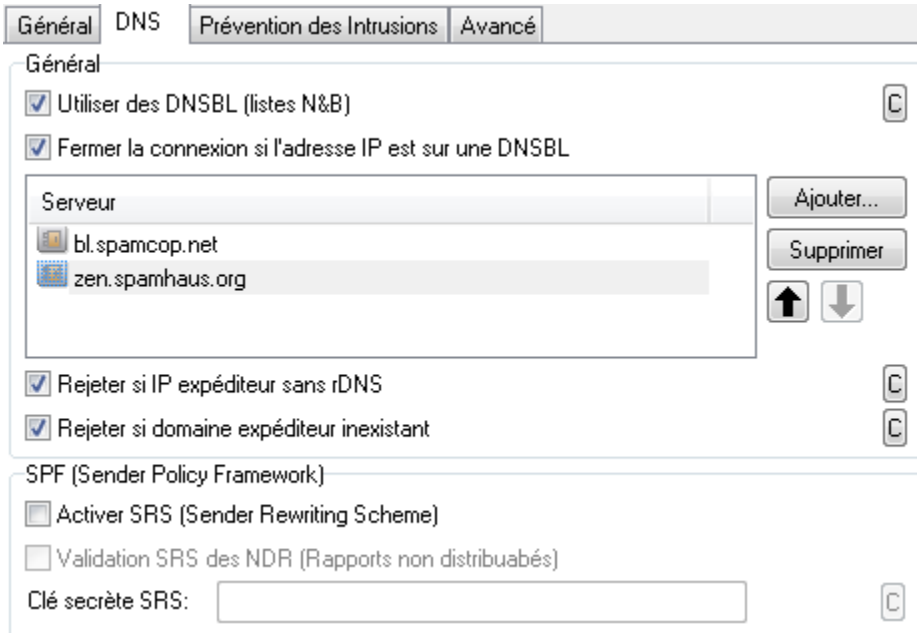
La liste des **Adresses IP et hôtes de confiance** doit contenir au minimum, l'adresse interne du serveur (127.0.0.1 - pour le Client Web). Il faut rajouter les adresses des sites qui envoient des messages mais qui ne peuvent pas s'authentifier : cela arrive quelquefois pour des automates d'émission qui ne prévoient pas de mémoriser un compte valide et son mot de passe.

La **configuration conseillée** est la suivante :

- pour le **serveur** (voir l'écran ci-dessus), cocher uniquement l'option : **Rejeter émetteur non autorisé...**
- pour le client **type Outlook**, positionner systématiquement **l'authentification SMTP**. Même si elle n'est pas forcément nécessaire, cela évitera des problèmes de connexion.

Paramètres DNS

Ces paramètres sont accessibles dans le menu Email -> Sécurité -> onglet DNS :



Les options indiquées dans l'écran ci-dessus sont conseillées.

L'objectif des **DNSBL** est de rejeter l'expéditeur dont l'origine est dans des listes noires de domaines. Il faut indiquer deux ou trois serveurs au maximum pour ne pas pénaliser les temps d'accès.

Le rejet des adresses IP non prévues pour le domaine (**expéditeur sans rDNS**) peut être coché, mais si certains domaines n'ont pas de rDNS et doivent quand même être acceptés, il faut alors les mettre en contournement. La détection de ce cas se traduit par un message SMTP du type :

501 5.7.1 <astigmatismslnc63@a1-med.de>... Sender IP must resolve

Certains domaines d'expéditeurs ne correspondent à aucune adresse IP. Seuls des spammeurs utilisent ce genre de domaines, il est donc conseillé de cocher l'option "**Rejeter si domaine expéditeur inexistant"**. La détection de ce cas se traduit par un message SMTP du type :

501 5.7.1 <root@ds130.ptyhost.com>... Sender domain must exist

L'option SPF qui n'autorise que les IP explicitement autorisées à émettre pour le domaine peut être validée dans le menu anti Spam.

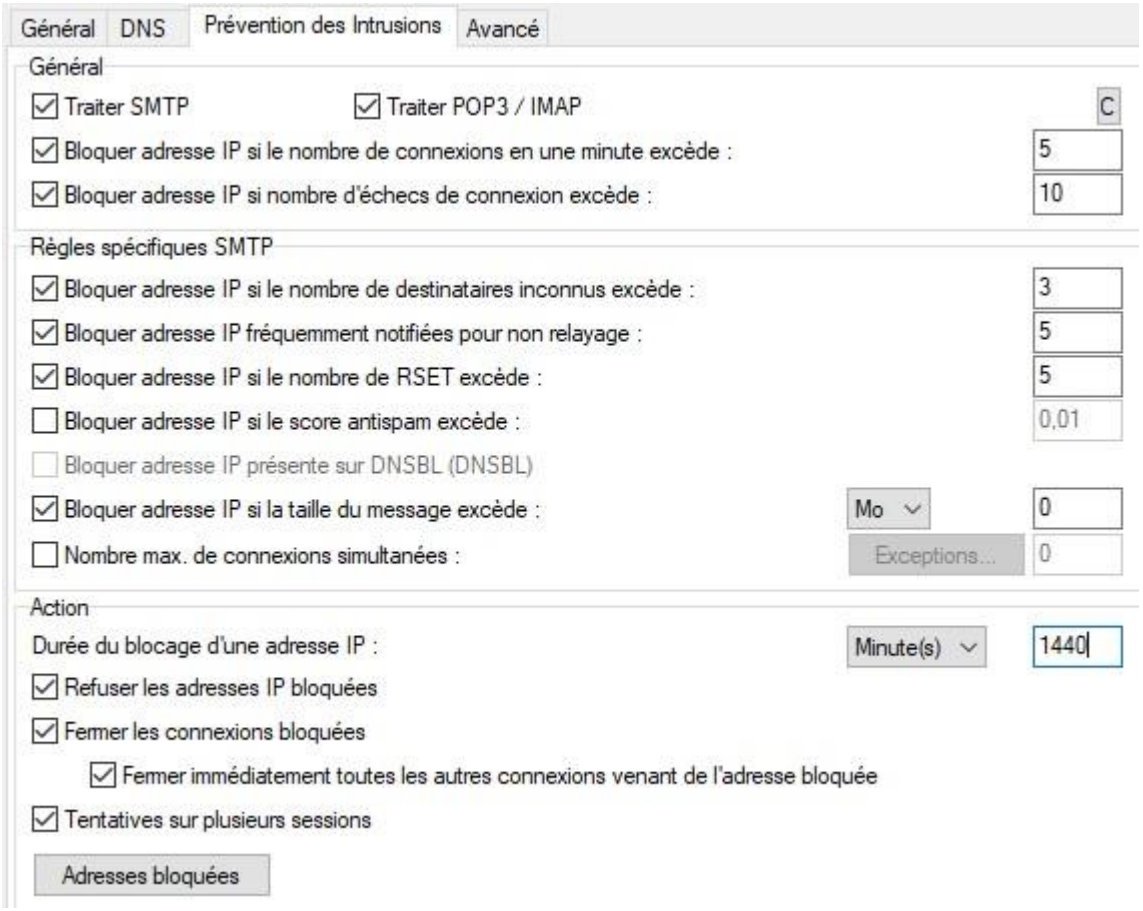
La fonction SRS permet l'utilisation par le destinataire de la fonction SPF. Elle n'est pas comprise par tous les serveurs. Si un serveur est dans ce cas, plutôt que de supprimer l'option, il vaut mieux le placer dans la table de contournement associée. La clé secrète est une chaîne de caractères quelconque.

Tous ces contrôles ne s'effectuent toutefois que si l'expéditeur n'est pas authentifié. Si l'expéditeur est authentifié, le domaine est toujours accepté.

La prévention des intrusions

Les tentatives provenant d'une adresse IP peuvent être limitées de façon à rejeter au plus vite les connexions dont on pense qu'elles sont abusives.

Ces paramètres sont accessibles dans le menu Email -> Sécurité -> onglet Prévention des intrusions :



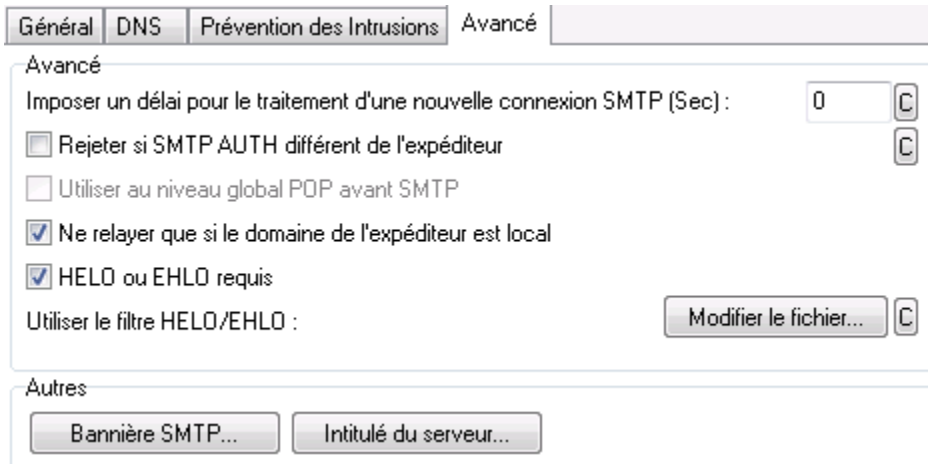
Les **options indiquées dans l'écran ci-dessus sont conseillées**.

La prévention des intrusions peut être activée sur les protocoles POP3 et IMAP. C'est une option utile, des attaques sur ces protocoles peuvent apparaître.

Cette option provoque une erreur de type :
421 4.0.0 Intrusion prevention active for [192.168.0.229]

Paramètres Avancés

Ces paramètres sont accessibles dans le menu Serveur de messagerie -> Sécurité -> onglet Avancé :



- Le **délai** pour le traitement d'une nouvelle connexion peut s'avérer nécessaire si des attaques en déni de service apparaissent. Il n'est en général pas utile.

- "**Rejeter si SMTP AUTH différent de l'expéditeur**" : cette option permet de rejeter un expéditeur qui s'authentifie avec un compte différent de son adresse mail; autrement dit, l'adresse mail de l'expéditeur est différente de l'adresse mail du compte d'authentification. Cette option impose plus de cohérence aux adresses mail mais n'apporte pas une sécurité supplémentaire très importante. Il provoque une erreur du type :
  501 5.7.1 <user@domaine.com>... Permission denied

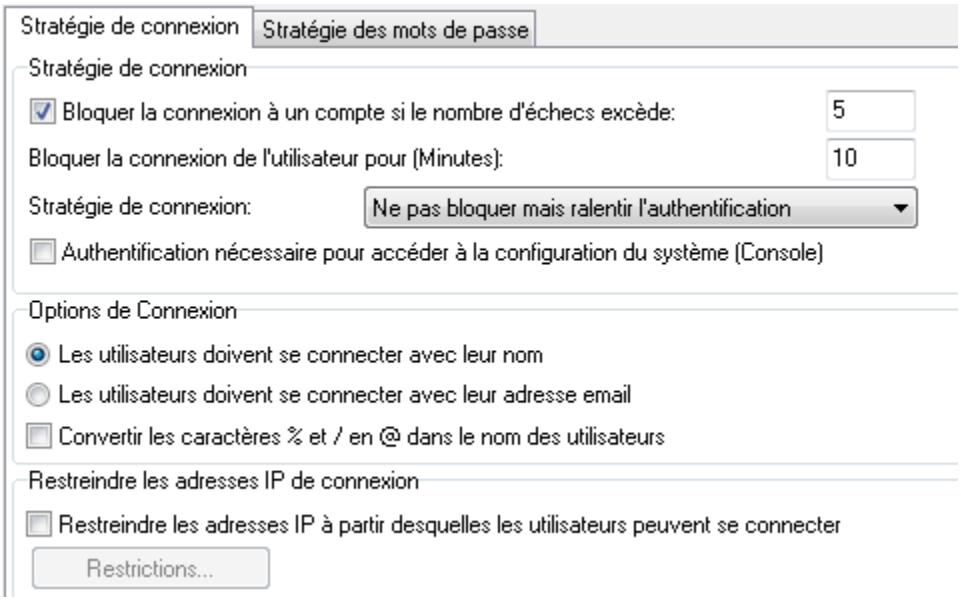
- "**Ne relayer que si le domaine de l'expéditeur est local**", cette option n'a d'effet que si l'expéditeur n'est pas authentifié. Il est conseillé de la cocher.

- "**Utiliser le filtre HELO ou EHLO**" permet de rejeter ou accepter certains serveurs de messagerie. La syntaxe du fichier est donnée dans la fenêtre.

La stratégie de connexion et des mots de passe

Ces contrôles sont accessibles par le menu Domaines et comptes -> Stratégies. Ils permettent de renforcer la sécurité d'accès des utilisateurs au serveur.

Stratégie de connexion

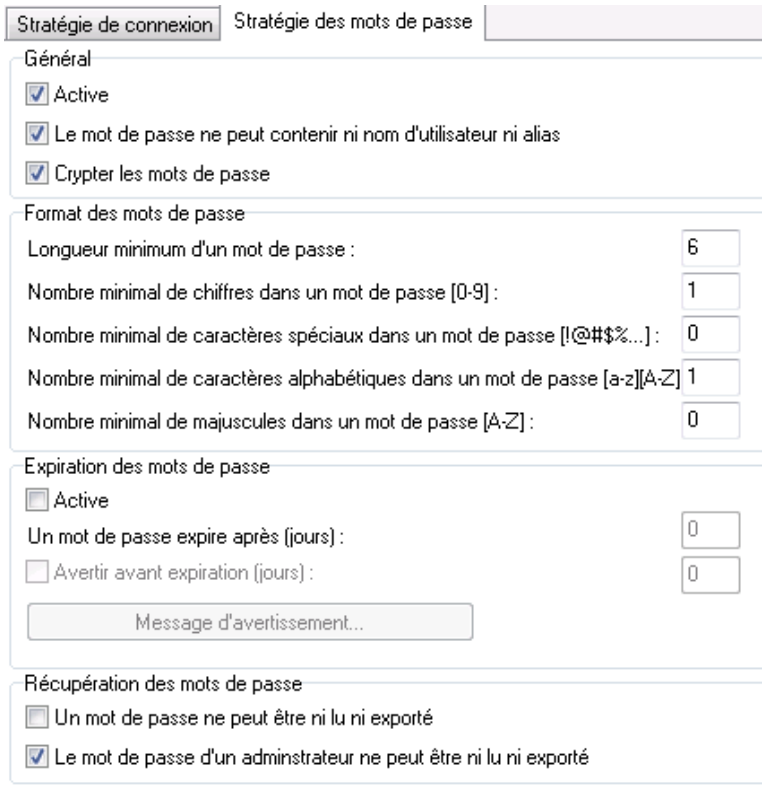


Le **blocage des comptes** permet d'éviter la recherche automatique des mots de passe par des robots mais il faut bien expliquer aux utilisateurs les conséquences d'un oubli.

L' "Authentification nécessaire pour accéder à la configuration du système" peut être utile si beaucoup d'utilisateur ont accès au serveur.

Connexion avec l'adresse mail (plutôt qu'avec le nom seul) : cette option peut éviter des ambiguïtés mais n'apporte pas de sécurité réelle. Elle s'applique aussi bien à l'authentification POP qu'à l'authentification SMTP. Elle s'applique aussi au Client Web (sauf spécification contraire dans GroupWare -> Client Web).

Stratégie des mots de passe



Le contrôle des mots de passe est indispensable car ceux-ci constituent le cœur de la sécurité du système. Il faut cependant trouver un compromis entre la "**dureté**" des mots de passe et son acceptation par les utilisateurs. C'est donc une politique à déterminer et à expliquer aux utilisateurs.

Le **cryptage** des mots de passe : ils ne sont pas cryptés en standard, ils sont donc en clair dans la base de données et consultables par les administrateurs du système. Si ces informations ne sont pas suffisamment protégées, il peut être plus sûr de les crypter.

Le mot de passe peut être renvoyé à un utilisateur à sa demande (option du Client Web) si l'option est autorisée par l'administrateur et si l'option "Un mot de passe ne peut être ni lu ni exporté" n'est pas cochée.

Pour **illustrer les risques**, certains robots essayent systématiquement une série de couples (plusieurs milliers) de cette façon sur le port POP3 :

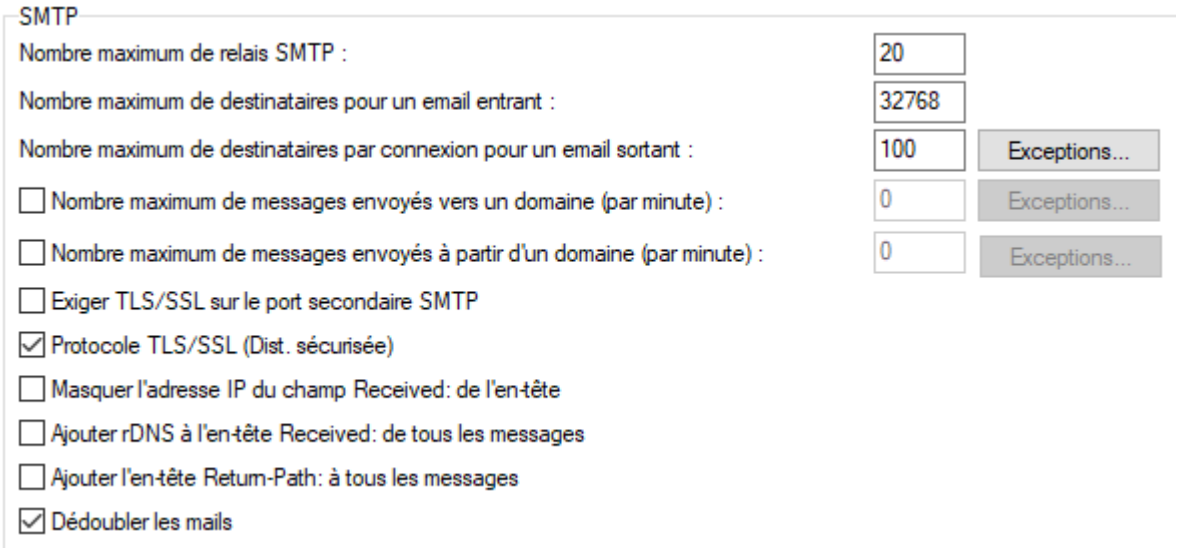
216.127.170.50 [08A0] 00:00:03 Connected
216.127.170.50 [08A0] 00:00:03 >>> +OK secosys.dnsalias.org IceWarp 10.1.2 POP3 ...
216.127.170.50 [08A0] 00:00:03 <<< USER admin
216.127.170.50 [08A0] 00:00:03 >>> +OK admin
*216.127.170.50 [08A0] 00:00:03 <<< PASS *********
216.127.170.50 [08A0] 00:00:06 >>> -ERR Unknown user or incorrect password
216.127.170.50 [08A0] 00:00:06 <<<
216.127.170.50 [08A0] 00:00:06 >>> -ERR Command unrecognized: ""
216.127.170.50 [08A0] 00:00:06 >>> -ERR Command unrecognized: ""
216.127.170.50 [08A0] 00:00:06 Disconnected

Lorsqu'un couple est découvert, il suffit de se servir du serveur comme relais pour envoyer des Spams.

Le cryptage SSL pour la distribution des messages

Cette option est accessible dans Email -> Général -> onglet Avancé.

Il s'agit ici de la **connexion entre IceWarp et le serveur distant** ("Client session") et non de la connexion entre l'utilisateur et le serveur, cette dernière est traitée dans le chapitre sur la sécurité vue de l'utilisateur.



Si la case "Protocole TLS/SSL" est cochée, IceWarp essaye de créer un dialogue crypté avec le serveur destinataire protégeant ainsi le contenu des messages contre l'écoute et l'intrusion. Si le distant ne peut établir la connexion SSL, elle est établie en mode normal. **Cette option est fortement conseillée**.

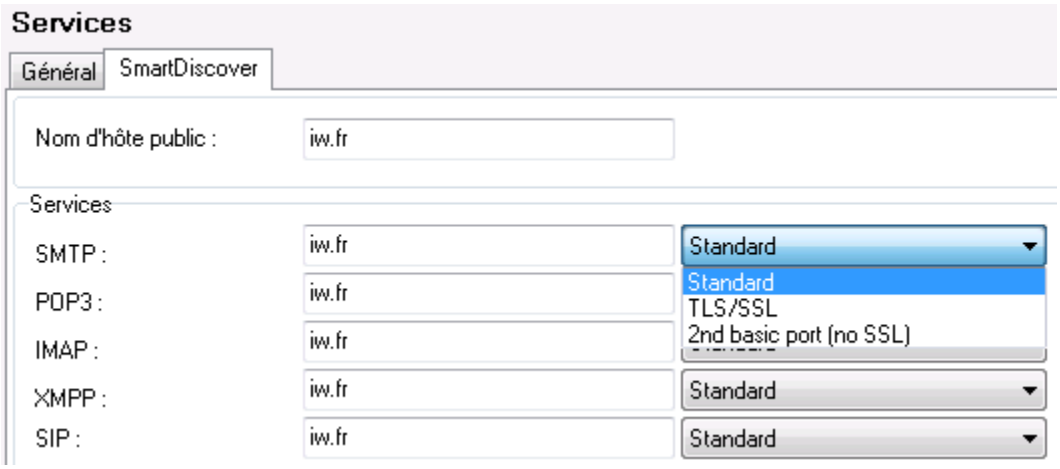
Un certificat qui n'a pas pu être vérifié pendant l'échange SMTP se traduit par un message du type :

Client session SSL: Not verified (6) - proceed anyway

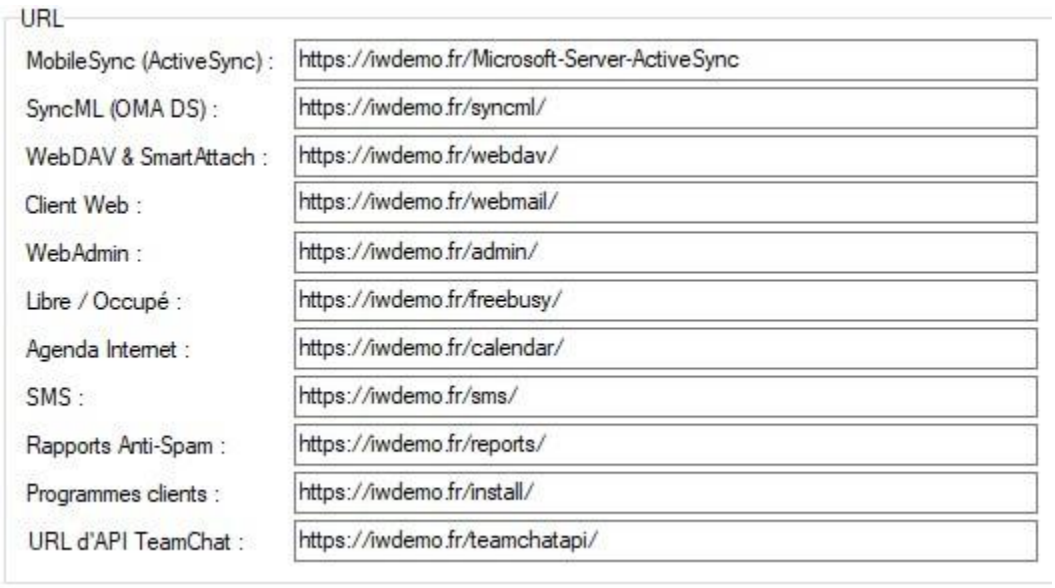
mais l'échange est quand même crypté.

Note : il faut que "Activer SSL/TLS" soit coché dans Système -> Avancé -> onglet Protocole.

Il est possible de forcer le mode de fonctionnement par protocole dans Système -> Services -> onglet SmartDiscover :

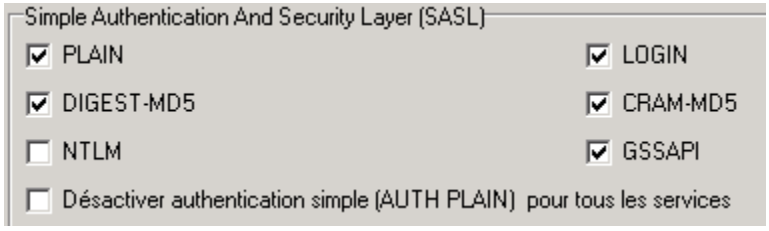


Dans ce même onglet, il est préférable de mettre tous les services en mode https (vérifier que le certificat est valide) :



Le cryptage des mots de passe

Dans Système -> Avancé -> onglet Protocole il y a possibilité de sélectionner les types d'authentifications qui peuvent être utilisés par le serveur :



Les deux premières méthodes (Plain et Login) transmettent le mot de passe en clair sauf si le protocole est en mode SSL/TLS.

Le serveur cherchera toujours à utiliser la solution la plus sûre parmi celles proposées par le client.

Pour la sécurité, le mieux serait de cocher "Désactiver l'authentification simple..." mais il faut s'assurer que tous les clients peuvent utiliser une des autres méthodes ce qui n'est pas toujours le cas.

Si cette option est cochée, le Client Web ne peut pas faire l'authentification SMTP (mais la connexion http a été authentifiée), il faut donc :

- Mettre l'adresse locale en hôte de confiance (dans Email -> Sécurité, il suffit en général de mettre 127.0.0.1)
- Ne pas utiliser l'authentification SMTP pour le Client Web (Groupware -> Client Web)

Si le serveur n'implémente pas l'authentification **GSSAPI**, il est préférable de la décocher pour éviter des erreurs d'authentification.

Les certificats

Il est indispensable d'avoir des certificats valides et certifiés par une autorité de certification.

Les certificats sont traités dans la console d'administration dans le menu Système -> Certificats.

Des informations détaillées sont données dans l'aide en ligne.

Le document suivant donne les détails pour créer un certificat :

http://www.icewarp.fr/download/guides/IceWarp%20-%20V11%20-%20Installation%20Certificat.pdf

Les protocoles SSL/TLS

Des variables API permettent d'affiner l'utilisation des protocoles dans les échanges cryptés.

Il faut aller sur la console d'administration dans Fichier -> Console API

Mettre Ext_SSL dans le filtre et on obtient les variables suivantes avec la valeur conseillée et le commentaire.

Nom : c_system_adv_ext_sslservermethod

Valeur : 0

Commentaire : Supported Server SSL Protocol. 0 - Default (currently the same as 4; but will be increased in future according to the actual security trends), 1 - Deprecated (the same as 3), 2 - Deprecated (the same as 3), 3 - Support SSL3 and newer (SSL3;TLS1;TLS1.1;TLS1.2), 4 - Support TLS1 and newer (TLS1;TLS1.1;TLS1.2), 5 - Support TLS1.1 and newer (TLS1.1;TLS1.2), 6 - Support TLS1.2 and newer (TLS1.2) - same as 5 on Linux RHEL5 and RHEL6

Nom : c_system_adv_ext_sslclientmethod

Valeur : 0

Commentaire : Supported Client SSL Protocol. 0 - Default (currently the same as 4; but will be increased in future according to the actual security trends), 1 - Deprecated (the same as 3), 2 - Deprecated (the same as 3), 3 - Support SSL3 and newer (SSL3;TLS1;TLS1.1;TLS1.2) (Client will send out TLSv1 client hello messages including extensions and will indicate that it also understands TLSv1.1;TLSv1.2 and permits a fallback to SSLv3), 4 - Support TLS1 and newer (TLS1;TLS1.1.TLS1.2) (Client will send out TLSv1 client hello messages including extensions and will indicate that it also understands TLSv1.1; TLSv1.2), 5 - Support TLS1.1 and newer (TLS1.1;TLS1.2) (Client will send out TLSv1.1 client hello messages including extensions and will indicate that it also understands TLSv1.2), 6 - Support TLS1.2 and newer (TLS1.2) (Client will send out TLSv1.2 client hello messages) - same as 5 on Linux RHEL5 and RHEL6

Nom : c_system_adv_ext_sslcipherlist

Valeur :
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS

Commentaire : List of supported ciphers according to (http://www.openssl.org/docs/apps/ciphers.html#)

Nom : c_system_adv_ext_sslhonorcipherorder

Valeur : vrai

Commentaire : When choosing a cipher, use the server's preferences instead of the client preferences (SSL_OP_CIPHER_SERVER_PREFERENCE in https://www.openssl.org/docs/ssl/SSL_CTX_set_options.html)

La sécurité vue de l'utilisateur

Il s'agit ici de traiter de la sécurité telle que la perçoit l'utilisateur, c'est à dire celle relative à la confidentialité de ses propres informations vis à vis de l'extérieur en général et des autres utilisateurs du serveur en particulier.

Nous indiquons systématiquement les options qu'il est conseillé de valider. C'est à l'administrateur de fixer les règles à appliquer et de les communiquer aux utilisateurs.

La sécurité avec les clients de type Outlook

Nous traitons ici des clients **Outlook** et **Thunderbird** mais les problèmes sont très similaires sur d'autres clients.

Le client dialogue avec le serveur par les protocoles POP ou IMAP pour la réception des messages et par le protocole SMTP pour l'émission des messages vers le serveur.

La réception et l'envoi de messages sont associés à plusieurs mécanismes de sécurité :

- **L'authentification** par nom d'utilisateur et mot de passe - toujours obligatoire pour lire des comptes POP ou IMAP.
- La possibilité de s'authentifier lors de **l'émission** d'un message (protocole SMTP)
- La possibilité d'échanger sur un canal crypté (**SSL**) pour la réception des mails (POP/IMAP) et/ou pour l'émission des mails (SMTP).
- Le cryptage et la mémorisation du **mot de passe** d'authentification.
- La possibilité d'envoyer et de recevoir des **messages cryptés/signés** par un certificat.

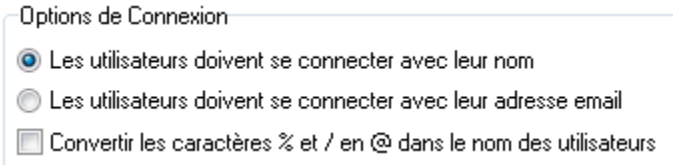
Authentification de l'utilisateur

Authentification pour la réception des messages

L'authentification par un couple **nom/mot de passe** est toujours obligatoire pour recevoir ses messages.

Ce couple doit être suffisamment sûr pour qu'il ne puisse pas être deviné. Voir le § sur la stratégie des mots de passe.

Le nom doit être remplacé par l'adresse mail complète si l'option "Connexion avec l'adresse mail" est positionnée dans la console d'administration "Domaines et comptes -> Stratégies -> onglet Stratégie de connexion ":



Cette option peut éviter des ambiguïtés mais n'apporte pas de sécurité réelle. Elle s'applique aussi bien à l'authentification POP qu'à l'authentification SMTP.

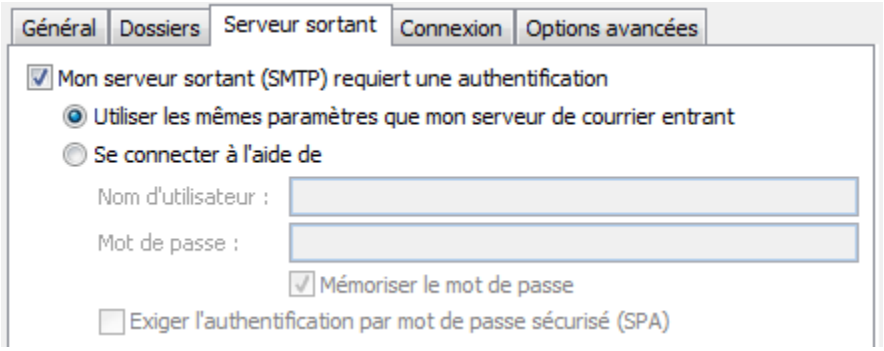
Authentification pour l'envoi des messages

Les serveurs peuvent demander à ce que l'émission des messages soit effectuée par un utilisateur authentifié mais ce n'est pas obligatoire.

L'absence d'authentification SMTP dans le client peut aboutir à une erreur du type :
550 5.7.1 <user1@domaine1>... we do not relay <user2@domaine2>

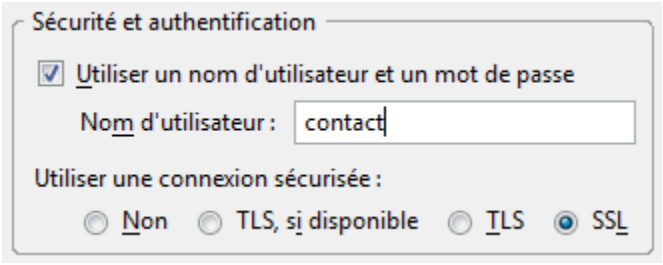
Nous conseillons donc de positionner systématiquement **l'authentification de l'échange SMTP** sur le client. Cette authentification s'effectue de la manière suivante.

Sur Outlook, il s'effectue dans les paramètres avancés du compte :



L'option "Utiliser les mêmes paramètres que mon serveur de courrier entrant" est valable si le compte POP et le compte SMTP sont communs, sinon, il faut donner explicitement les paramètres du compte SMTP.

Sur Thunderbird dans la description du serveur SMTP:



Le mot de passe est demandé lors de la première session.

Connexion SSL

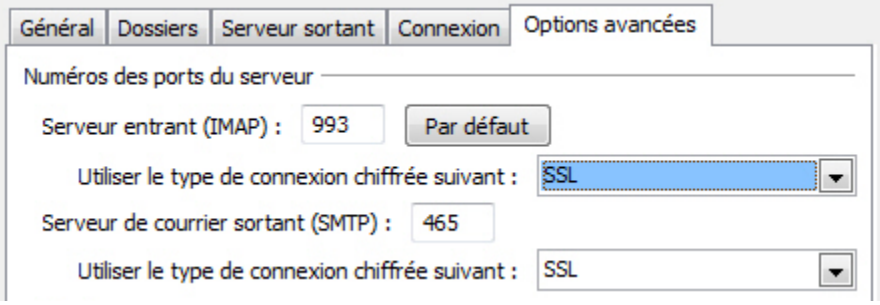
La connexion SSL permet le cryptage des échanges entre le client et le serveur donc évite l'écoute et l'intrusion. **Cette option est fortement conseillée** si la liaison entre le client et le serveur n'est pas dans un bâtiment protégé.

La connexion SSL peut être positionnée ou non dans le client.

Elle nécessite la présence d'un certificat valide dans le serveur IceWarp. Voir le § Certificat pour plus de précisions.

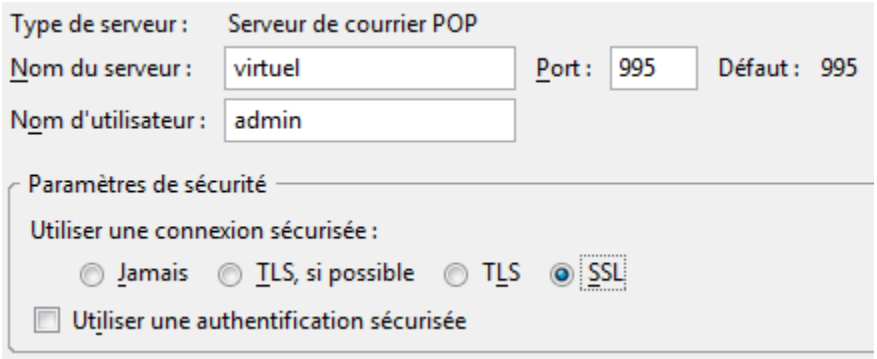
Positionnement du SSL dans Outlook

Dans les paramètres avancés du compte :

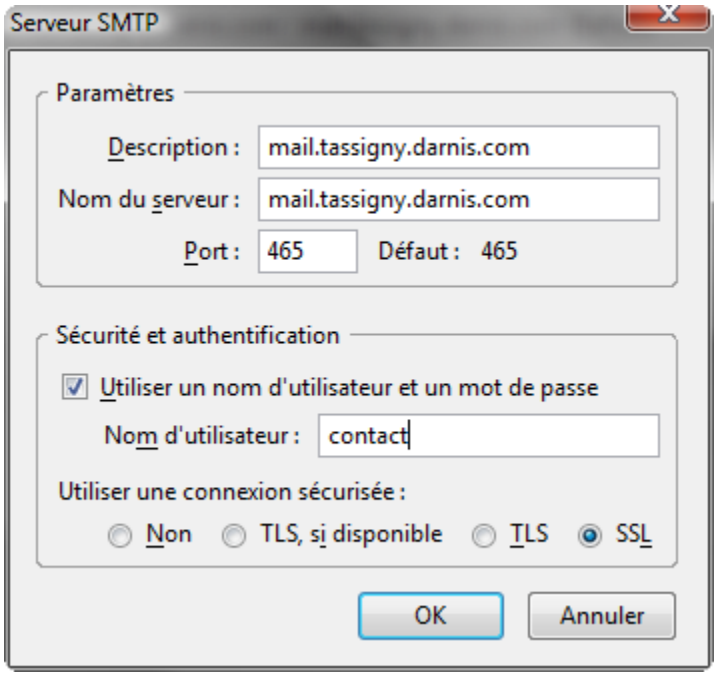


Positionnement du SSL dans Thunderbird

Dans les paramètres serveur du compte :



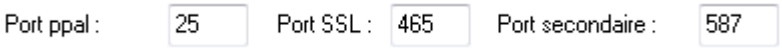
Dans les paramètres du serveur sortant (SMTP)



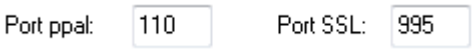
Ports utilisés par IceWarp

Attention : vérifier la coïncidence des ports du client avec ceux définis dans le service correspondant d'IceWarp (Système -> Services) :

SMTP



POP3



IMAP

Il faut aussi que ces ports soient ouverts sur les pare-feux du serveur et du routeur.

La sécurisation du mot de passe

Le mot de passe est, en standard, transmis en clair ce qui le rend vulnérable à l'écoute. Pour palier à cette faiblesse, certains clients proposent de le crypter :

- Transmission cryptée du mot de passe (SPA sur Oulook)).
- Authentification sécurisée (Thunderbird)

Ces options ne sont cependant pas acceptées par IceWarp mais la **connexion SSL** les rend inutiles puisqu'ils sont alors cryptés avec le reste de l'échange.

Cryptage/signature des messages

Cette fonction permet de protéger complètement les données transmises et reçues vis à vis de tous en dehors du destinataire des messages. Elle nécessite la création et le stockage de clés publique et privée pour chaque interlocuteur et la diffusion des clés publiques.

C'est une méthode très efficace mais difficile à mettre en œuvre, il faut consulter la documentation spécifique du client de messagerie utilisé. Pour le Client Web, le document de l'utilisateur donne la méthode à utiliser.

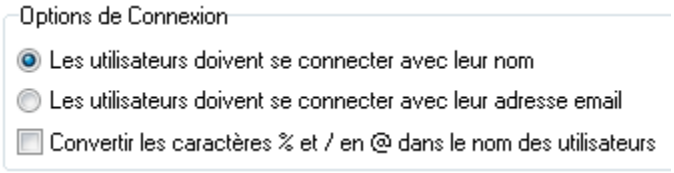
La sécurité avec le Client Web

Authentification de l'utilisateur

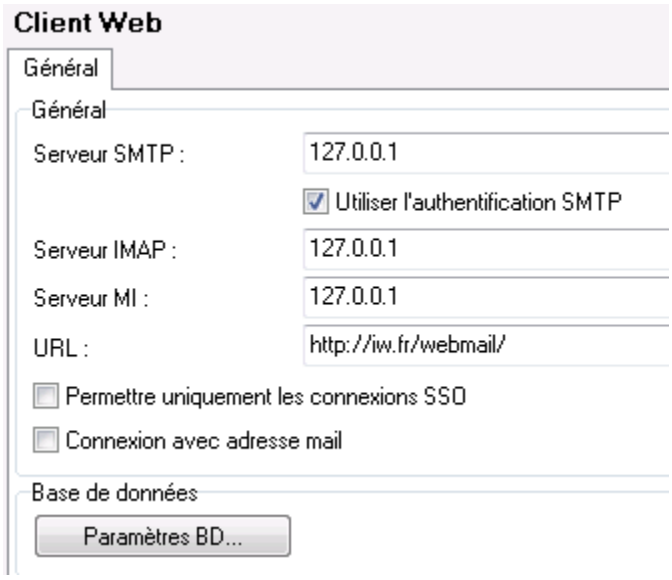
Le Client Web est vu comme un utilisateur local du serveur, il utilise le protocole IMAP (sur les comptes POP&IMAP) pour la synchronisation des dossiers et le protocole SMTP pour l'envoi des messages.

L'utilisateur doit toujours s'authentifier vis à vis du serveur par un couple **nom/mot de passe**.

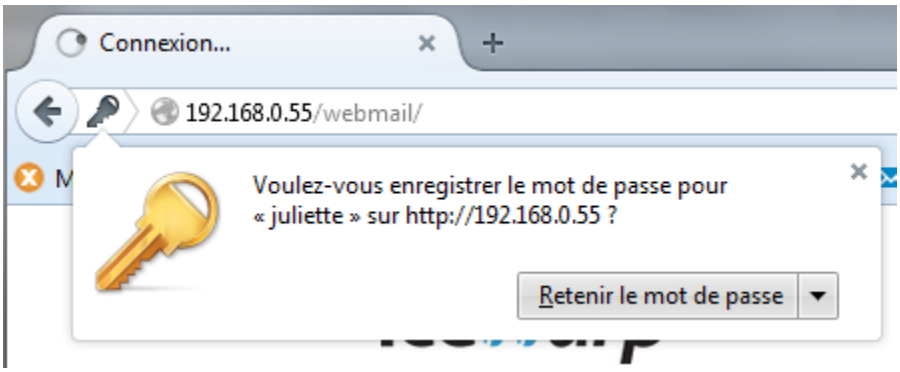
Le nom doit être remplacé par l'adresse mail complète si cela est imposé par l'option suivante de la console d'administration "Domaines et comptes -> Stratégies -> onglet Stratégie de connexion ":



Dans le **menu GroupWare -> Client Web** de la console d'administration, il est possible de cocher l'option "Connexion avec l'adresse mail". Dans ce cas, il est possible de se connecter aussi avec l'adresse mail :



Lors de la connexion, le navigateur demande à l'utilisateur s'il veut que le système mémorise ou non son mot de passe (ici FireFox) :



Il existe aussi l'option "Rester connecté" sur la page de login du Client Web. Il est **fortement déconseillé de mémoriser** l'utilisateur et le mot de passe sauf sur un ordinateur fixe et personnel.

Connexion SSL

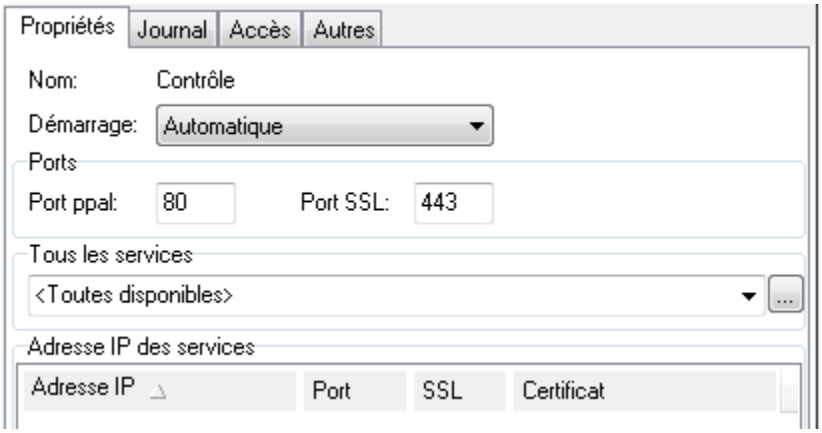
La transaction peut être ou non sécurisée par l'utilisation du protocole HTTPs. Ceci se définit au moment de la connexion.

Connexion **non sécurisée** : **http://<serveur>/** ou **http://<serveur>/webmail/**

Connexion **sécurisée** : **https://<serveur>/** ou **https://<serveur>/webmail/**

Dans ce cas, tous les échanges sont chiffrés et donc protégés contre l'écoute et l'intrusion.

Les ports sont définis dans le menu Système -> Services -> onglet Général -> service Web :

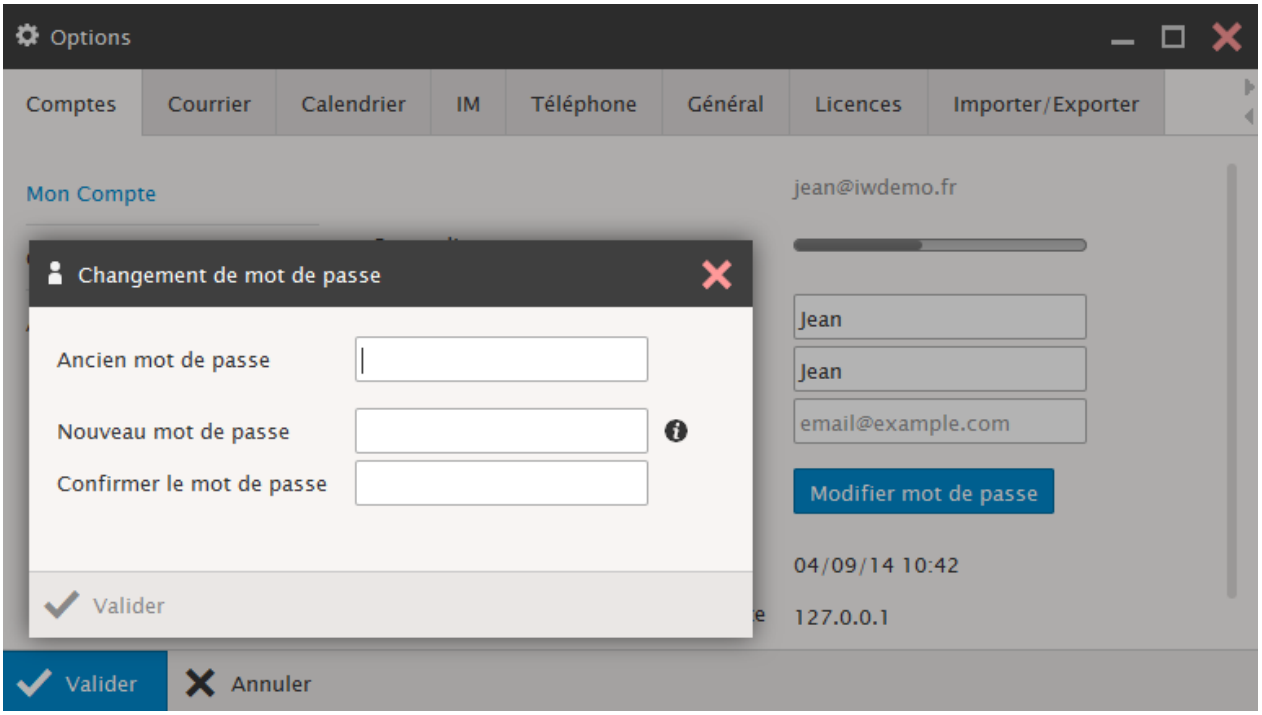


La solution sécurisée est nettement préférable mais le serveur ne peut pas l'imposer, elle reste **au choix de l'utilisateur.** Elle nécessite un certificat dans le serveur (voir le § sur les certificats).

Le changement du mot de passe

Le mot de passe doit être conservé secret et doit répondre à la stratégie des mots de passes définie pour tout le serveur (voir le § sur la sécurité du serveur).

Un utilisateur peut (et doit dans certains cas) changer son mot de passe dans le Client Web par l'écran suivant accessible par le menu Options -> Comptes -> Mon Compte :



Cryptage/signature des messages

Cette fonction permet de protéger complètement les données transmises et reçues vis à vis de tous en dehors du destinataire des messages. Elle nécessite la création et le stockage de clés publique et privée pour chaque interlocuteur et la diffusion des clés publiques.

Sa mise en œuvre pour le Client Web est décrite dans le document disponible en ligne dans le **menu Aide de ce Client**.