Infra Mail Orange

Points d'accès sécurisé

Mon but ici est de lister les **points d'accès sécurisé** à l'infra de mail d'Orange (Grand Public). La liste est définie à la fin de cette section

Orange comme la plupart des FAI met à disposition de leur client une infrastructure de messagerie électronique (Courriel / Mail / e-Mail / Etc.) répartie en 2 fonctions :

- Envoi / transfert de courriel :
  - Protocole SMTP / SMTPS
- Réception de courriel :
  - Protocole POP / POPS (en version 3, aka POP3)
  - Protocole IMAP / IMAPS

Chacun de ces protocoles sont disponibles sans chiffrement et surtout avec (SSL/TLS, STARTTLS).

Dans un monde parfait (En suivant les recommandations issues des RFC), les ports associés à chacun de ces protocoles sont :

Protocole	Port	Format des échanges	Usage
SMTP	25	Non chiffré	Ne pas utiliser !
SMTP	465	SSL/TLS	Déprécié
SMTP	587	STARTTLS	**Recommandé** avec STARTTLS uniquement
POP	110	Non chiffré + STARTTLS	**Recommandé** avec STARTTLS uniquement
POP	995	SSL/TLS	Déprécié
IMAP	143	Non chiffré + STARTTLS	**Recommandé** avec STARTTLS uniquement
IMAP	993	SSL/TLS	Déprécié

Testons donc rapidement ces points d'accès sur l'infra Mail d'Orange (On a besoin d'un **Linux** avec **OpenSSL**) afin de redéfinir un listing des ports et méthodes d'accès à cette infra...

Rappel des VIP d'accès aux services de messagerie d'Orange :

- SMTP : `smtp.orange.fr`
- POP : `pop.orange.fr`
- IMAP : `imap.orange.fr`

Résultat type et interprétation (issu d'openssl en mode client) :

- Port **fermé**

```
connect: Connection timed out
connect:errno=110
```

- Port **ouvert** mais **pas de support STARTTLS**

```
CONNECTED(00000003)
didn't found starttls in server response, try anyway...
140245429929624:error:140770FC:SSL routines:SSL23_GET_SERVER_HELLO:unknown
protocol:s23_clnt.c:794:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 233 bytes and written 340 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
...
---
```

- Port **ouvert** avec **support STARTTLS ou SSL/TLS**

```
CONNECTED(00000003)
...
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-SHA
...
```

Place aux tests...
Tests des **ports non chiffré ou avec STARTTLS**

```
echo "Q" | openssl s_client -connect smtp.orange.fr:25  -starttls smtp
echo "Q" | openssl s_client -connect smtp.orange.fr:587 -starttls smtp
echo "Q" | openssl s_client -connect pop.orange.fr:110  -starttls pop3
echo "Q" | openssl s_client -connect imap.orange.fr:143 -starttls imap
```

Tests des **ports chiffré avec SSL/TLS**

```
echo "Q" | openssl s_client -connect smtp.orange.fr:465
echo "Q" | openssl s_client -connect pop.orange.fr:995
echo "Q" | openssl s_client -connect imap.orange.fr:993
```

Ce qui donne comme résultat (Valable au 04/01/2018) pour le **FAI Orange**

Protocole	Port	Format des échanges	Recommandations
SMTP	25	Non chiffré	Ne pas utiliser ! JAMAIS
SMTP	465	SSL/TLS	**Recommandé**
SMTP	587	Non chiffré	Ne pas utiliser, car pas de support STARTTLS
POP	110	Non chiffré	Ne pas utiliser, car pas de support STARTTLS
POP	995	SSL/TLS	**Recommandé**
IMAP	143	Non chiffré + STARTTLS	**Recommandé** avec STARTTLS uniquement
IMAP	993	SSL/TLS	Déprécié

Le mot de la fin…
STARTTLS semble supporté uniquement sur l'IMAP mais un accès sécurisé **SSL/TLS est offert** pour **l'ensemble des services de courriel** (ce qui me parait plutôt normal d'un point de vue sécurité). En soit, le support de **STARTTLS** n'est pas indispensable, mais cela permettrait d'offrir du chiffrage sur les ports standard tout en respectant les préconisations portées par les RFC.

A titre personnel, je préfère ne pas utiliser STARTTLS et forcer les connexions en SSL/TLS, ce qui me garantie que les échanges sont chiffrés quoi qu'il arrive (pas de négociation possible), bien que je suppose que fait d'interdire tout échange non chiffré avec STARTTLS est un comportement paramétrable dans tout client mail digne ce nom (Quid de fetchmail ?).