

Le SMTP démystifié

Anthony Brodard, Devops @Sendinblue

Sommaire

- Rappels
- Description du protocole
- Hello world
- Mécanismes de lutte anti fraude
- Analyse & performance

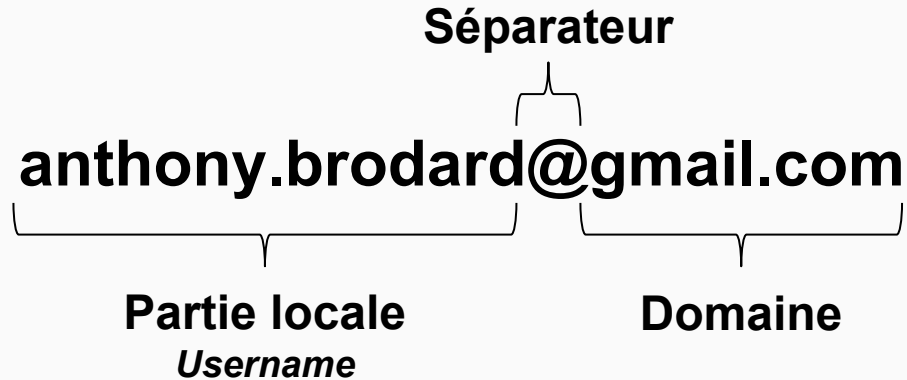
Rappel - Une adresse email

Séparateur

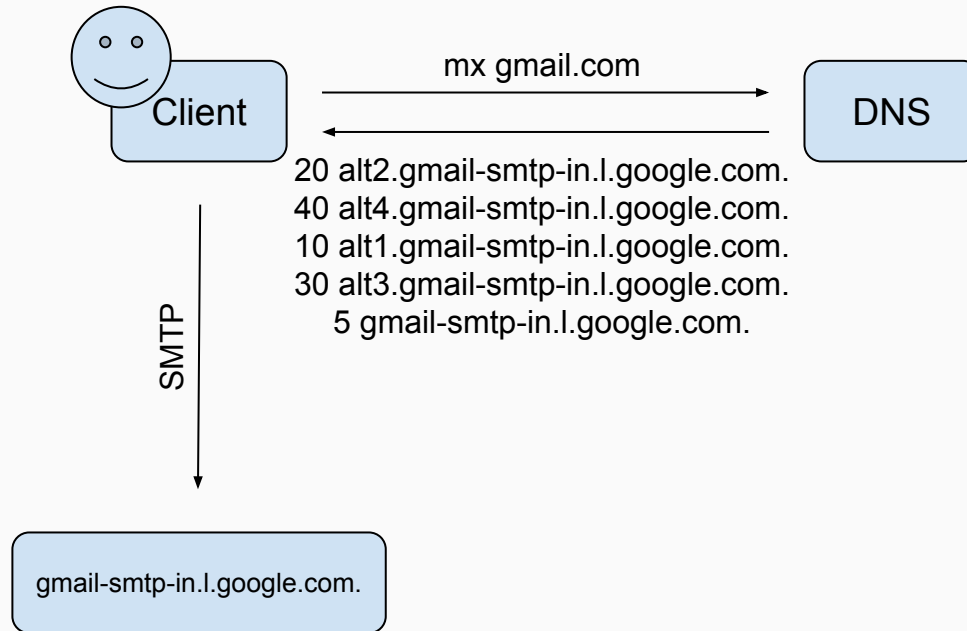
anthony.brodard@gmail.com

Partie locale
Username

Domaine

A diagram illustrating the components of an email address. The email address 'anthony.brodard@gmail.com' is centered. Above it, the word 'Séparateur' is written, with a bracket pointing to the '@' symbol. Below the address, two brackets are used to divide it into two parts. The left bracket is labeled 'Partie locale' with 'Username' written below it. The right bracket is labeled 'Domaine'.

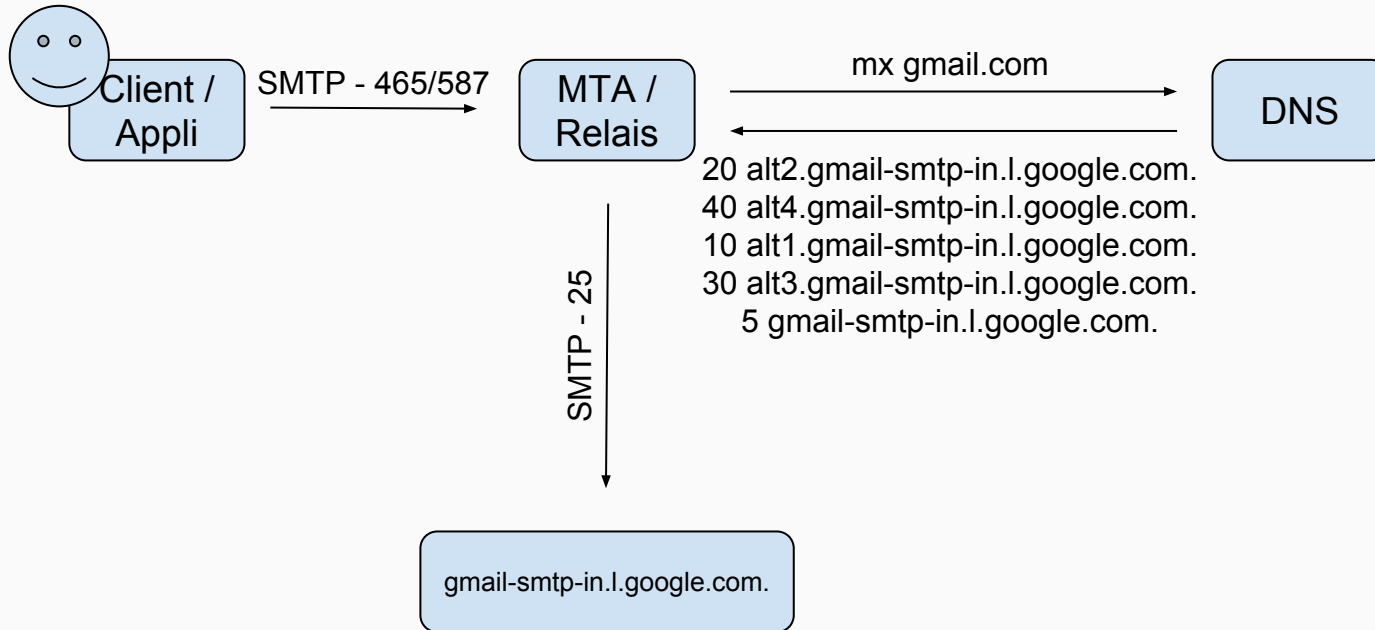
Envoi d'un email



Protocole SMTP

- Simple Mail Transfert Protocol
- 1ère version dans les années 80, v2 en 2008
- Ports : TCP/25 (inter MTA), TCP/465* (SMTPS), TCP/587 (Client)
- Robuste, faible dépendance au réseau
- Asynchrone et multi hop
- Pas d'authentification

Envoi d'un email



Hello World

```
telnet gmail-smtp-in.l.google.com. 25
EHLO mx.chatops.fr
MAIL FROM: <contact@chatops.fr>
RCPT TO: <anthony.brodard@gmail.com>
DATA
Subject: Hello World !
From: Chatops <contact@chatops.fr>
Hello World !
.
```

```
root@demo:~# telnet gmail-smtp-in.l.google.com. 25
Trying 64.233.184.27...
Connected to gmail-smtp-in.l.google.com.
Escape character is '^]'.
220 mx.google.com ESMTP j80si308898wmj.57 - gsmt
EHLO mx.chatops.fr
250-mx.google.com at your service, [51.255.200.139]
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
MAIL FROM: <contact@chatops.fr>
250 2.1.0 OK j80si308898wmj.57 - gsmt
RCPT TO: <anthony.brodard@gmail.com>
250 2.1.5 OK j80si308898wmj.57 - gsmt
DATA
354 Go ahead j80si308898wmj.57 - gsmt
From: Chatops <contact@chatops.fr>
To: Anthony Brodard <anthony.brodard@gmail.com>
Subject: Hello World
OrleansTech Demo
.
250 2.0.0 OK 1461515998 j80si308898wmj.57 - gsmt
quit
221 2.0.0 closing connection j80si308898wmj.57 - gsmt
Connection closed by foreign host.
```

Les politiques anti-fraude

- Comment lutter face à l'explosion des messages de spam et de fraude ?



Reverse DNS

- DNS corrects
 - Le EHLO (ou HELO) peut être résolu...
 - ... et la résolution inverse est correcte

```
root@demo:~# dig mx.chatops.fr +short
51.255.200.139
root@demo:~# dig -x 51.255.200.139 +short
mx.chatops.fr.
```

SPF (2006)

- Sender Policy Framework
- Indique quel serveur est autorisé à envoyer un email pour le domaine du MAIL FROM
- “Si le propriétaire du domaine l’autorise, c’est que cette IP peut envoyer”
- DNS : Type TXT (SPF déprécié)
- Format : “v=spf1 ip4:51.255.200.139/32 ~all”

```
root@demo:~# dig txt chatops.fr | grep spf1
chatops.fr.      3559    IN      TXT     "v=spf1 ip4:51.255.200.139/32 include:spf.sendinblue.com mx ~all"
root@demo:~#
```

DKIM (2008)

- DomainKey Identified Mail
- Evolution de DomainKey, proposée par Cisco et Yahoo!
- Signature de l'email par l'émetteur (clé privée), et diffusions de la clé publique dans les DNS
- Header DKIM-Signature
- DNS : Type TXT : {SELECTOR}._domainkey.{domain}

```
root@demo:~# dig txt mail._domainkey.chatops.fr +short  
"k=rsa;p=MIgfMA0GCSqGSIb3DQEBQUAA4GNADCBiQKBgQDeMVIzrCa3T14JsNY0IRv5/2V1/v2itlviLQBwXsa7shBD6TrBkswsFUToPyMFwC9tbR/5eyOnRBH0ZVxp+lsmTxi d2Y2z+FApQ6ra2VsXfbJP3HE6wA00YTV EJt1Tm  
eczHed2Jiz/fcabIISgXEdSpTYJhb0ct0VJRxcg4c8c7wIDAQAB"
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=chatops.fr;  
q=dns/txt; s=mail; bh=plpDfjpHble0DSUQ1uQ+b3PpE7TafHbI8XiPE0DWJCY=;  
h=from:subject:date:mime-version:content-type:content-transfer-encoding;  
b=16FkOYFE1oBPyc0iu+aZqlaNpAlUDqWcfSMwwDR5HP1mcSp9XA xwFecE065chewkFcrKkip2KxYP  
dBmLVJjCr lXi iF870Z5IkEgSAAd7v5ZK0kRkGeQi9030w0F8ZrcwTHLXw0CTm9F0xT+4BWET1Kuw  
ZFJzk6r7sdB31MLx10c=
```

DMARC (2012)

- Domain-based Message Authentication, Reporting and Conformance
- Indique quelles mesures prendre en cas de SPF et/ou DKIM fail
 - Fais le lien entre SPF et DKIM
 - None/Reject/Quarantine les emails
 - % d'emails à accepter
- Envoi d'un rapport journalier à l'adresse indiquée dans le DMARC
- Record DNS TXT : `_dmarc.{domain}`

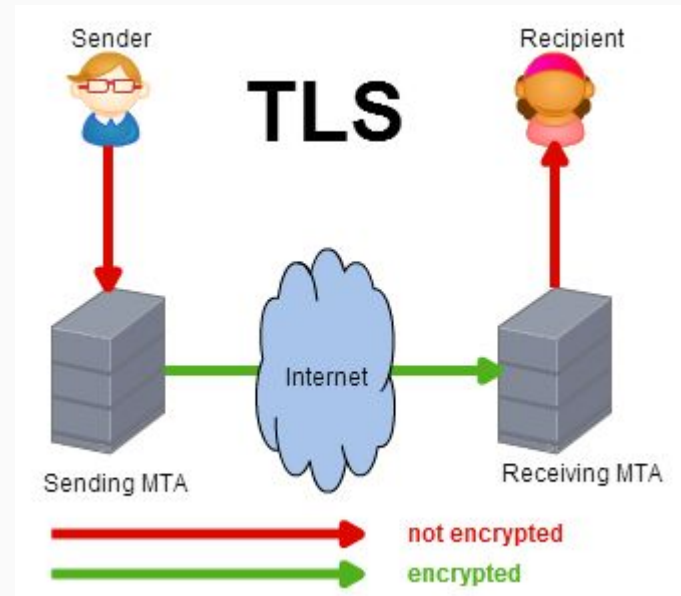
```
root@demo:~# dig txt _dmarc.chatops.fr +short  
"v=DMARC1; p=none; sp=none; rua=mailto:dmarc@mailinblue.com!10m; ruf=mailto:dmarc@mailinblue.com!10m; rf=afrf; pct=100; ri=86400"
```

ARC (2016 ?)

- Authenticated Received Chain
- Nouveau projet (10/2015) pour remplacer les lacunes de DMARC -> redirection et mailing-list
- Ajout de trois nouveaux headers
 - ARC-Seal
 - ARC-Message-Signature
 - ARC-Authentication-Results
- Encapsule le résultat de SPF + DKIM + DMARC

TLS

- Chiffrement des email en TLS
- De bout en bout ?
- Désormais “obligatoire” pour Gmail



Délivrabilité & Réputation

Le respect des normes ne garantie pas la délivrabilité -> Réputation + contenu entrent en jeu

La réputation change en fonction du destinataire (gmail, microsoft...). Chacun à sa propre politique !

Quelques bonnes pratiques :

- Chauffer les IPs
- Eviter les mots clés de SPAM (viagra, enlarge, porn, medic, bank...)
- Adresses Opt-in + consentement (non partenaire) / Eviter les spam trap

Analyse et performance

[Mxtoolbox](#) (détection blacklist IP / checklist configuration)

[Port25 Verifier](#)

Les outils postmaster des FAI

Ressources

- SMTP -> RFC 788, 821, 2821, 5321
- SPF -> RFC 4408, 7208 | <http://www.openspf.org/>
- DKIM -> RFC 6376 | <http://www.dkim.org/>
- DMARC -> RFC 7489 | <https://dmarc.org/>
- ARC -> <http://arc-spec.org/>

Des questions ?