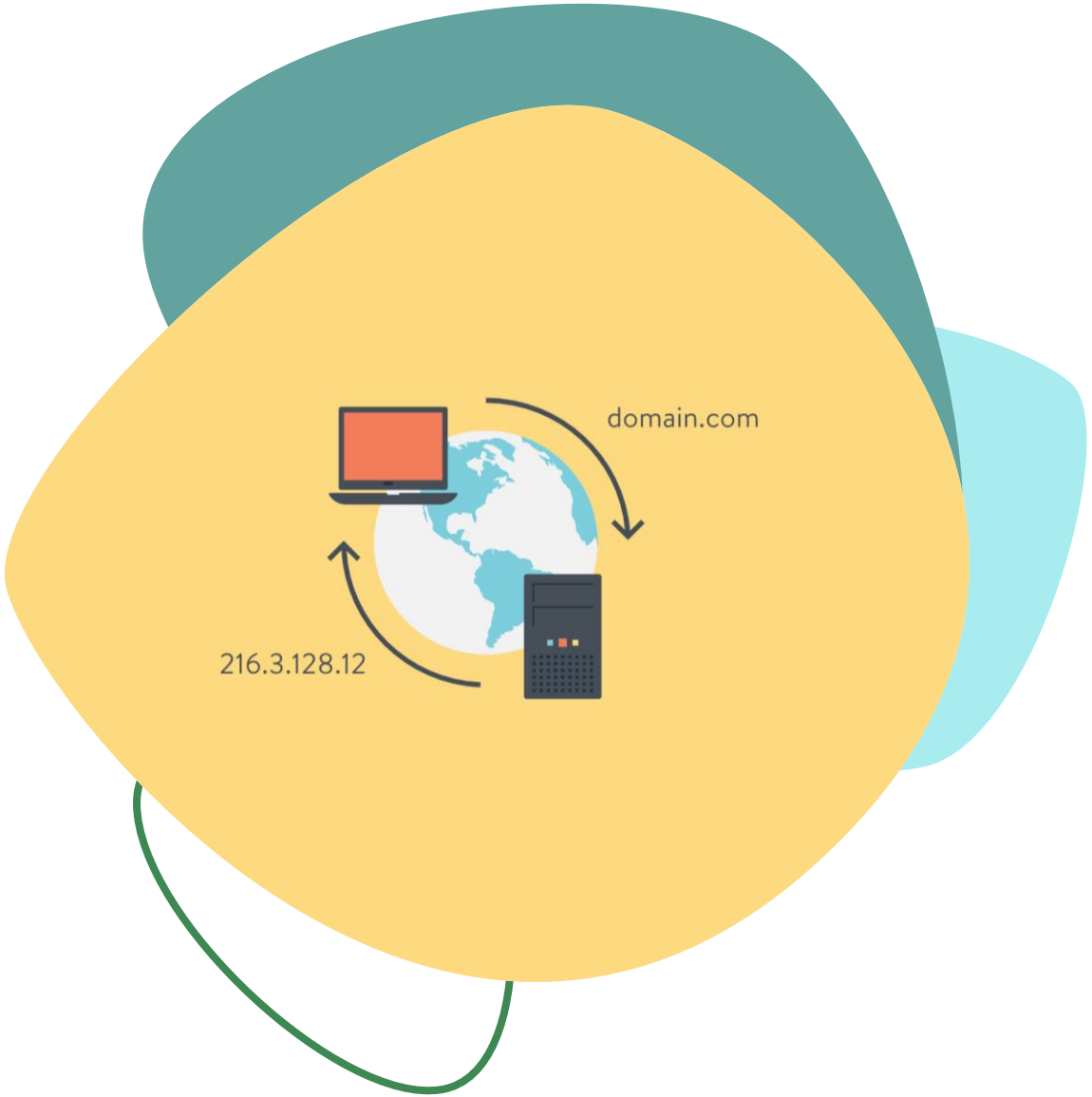
# Les enregistrements DNS



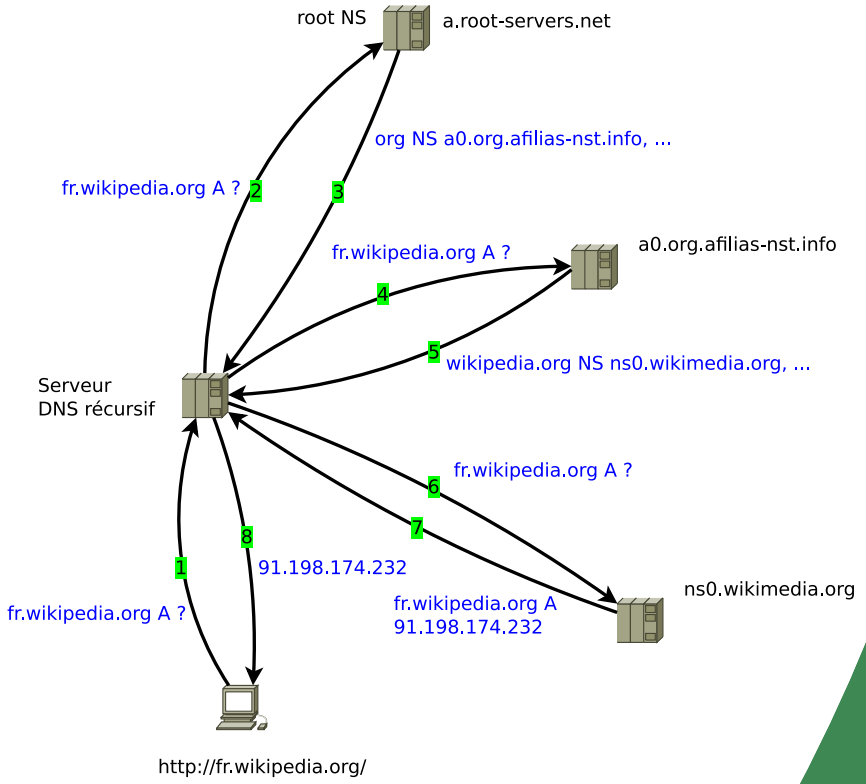

**26 mars 2024**
**Polytech Dijon – semestre 6**

Paul DUCOLOMB, Firmin LAUNAY, Théophile REY


# Sommaire

- Généralités sur les DNS
- Présentation & démonstration des enregistrements
- Attaques sur les DNS

POLYTECH DIJON

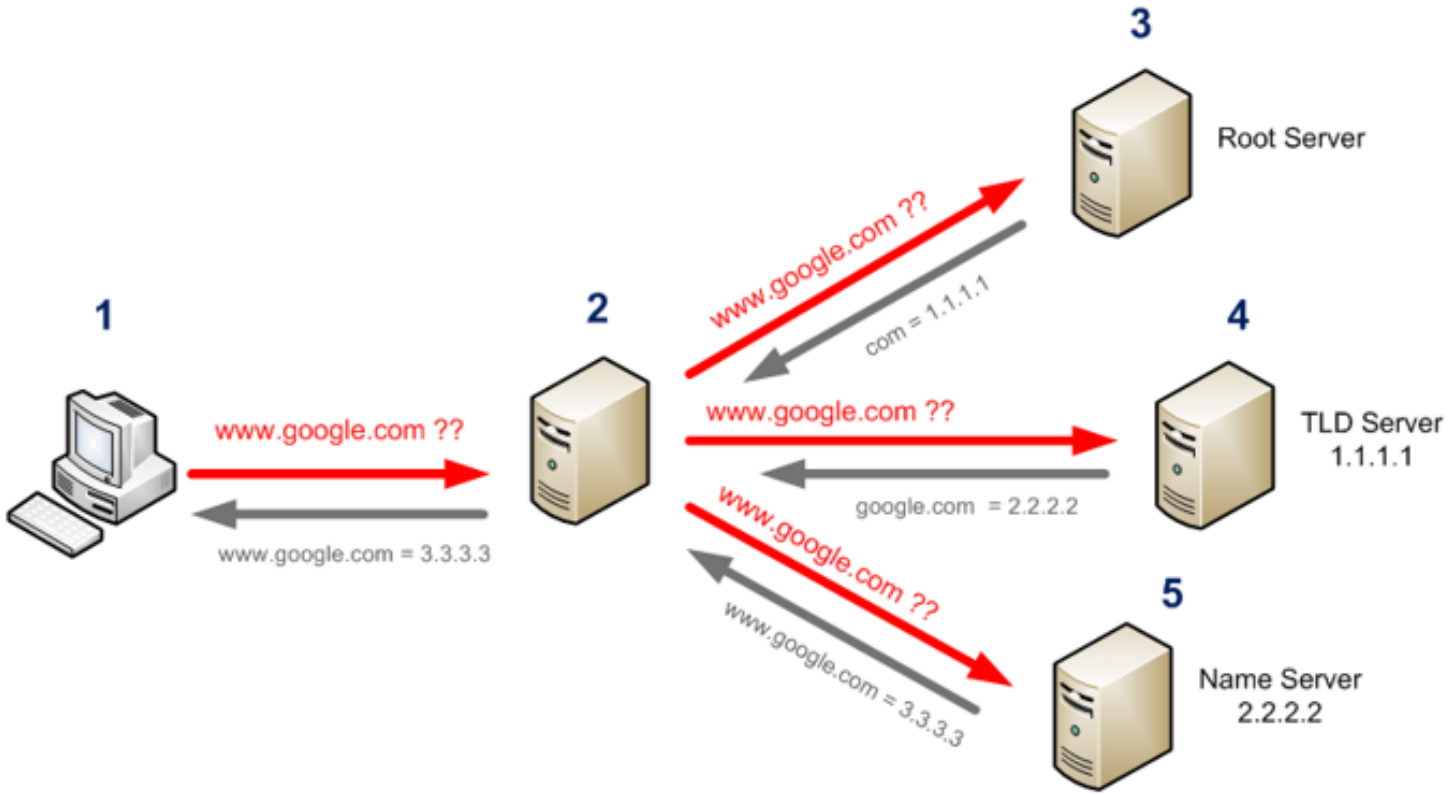



# Généralités sur les DNS

Définitions, rappels

POLYTECH DIJON

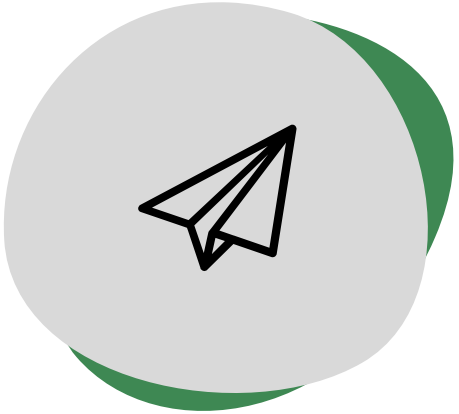
# À quoi servent les serveurs DNS ?



# Propagation et réplication DNS

**Serveur d'autorité**

Propre à chaque TLD, à chaque domaine, ...



**Propagation**

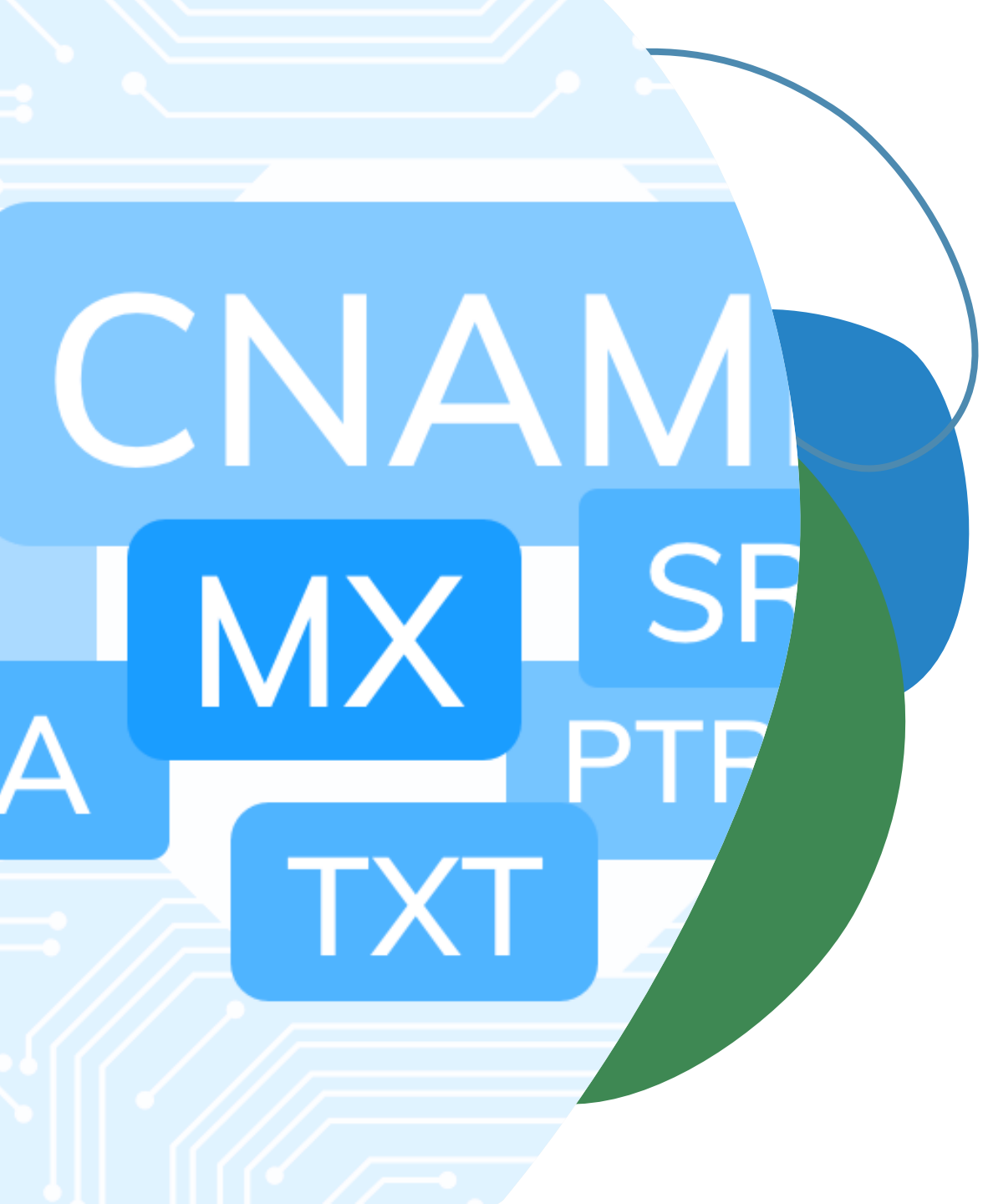
Les autres DNS sont informés du changement

**Réplication...**

Les DNS grand public répliquent généralement ces changements

**... ou pas !**

Certains DNS ne répliquent pas ces changements pour diverses raisons




# Enregistrements DNS

Présentation, démonstration

POLYTECH DIJON

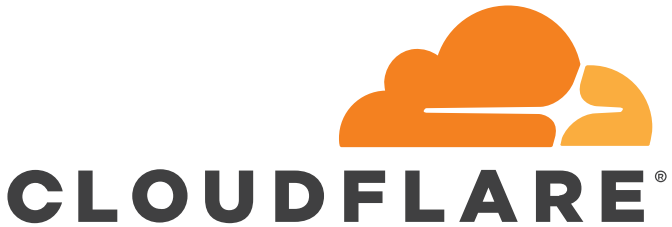
# Quelques types d'enregistrement DNS

- **A** : Mappage d'un nom de domaine à une adresse IPv4
- **AAAA** : Mappage d'un nom de domaine à une adresse IPv6
- **CNAME** : Mappage d'un nom de domaine à un autre nom de domaine
- **MX** : Acheminement des courriels entrants pour un domaine
- **TXT** : Association au domaine d'informations sous forme de texte
- **LOC** : Association au domaine d'une position physique 🤡

# Entités pour notre démo

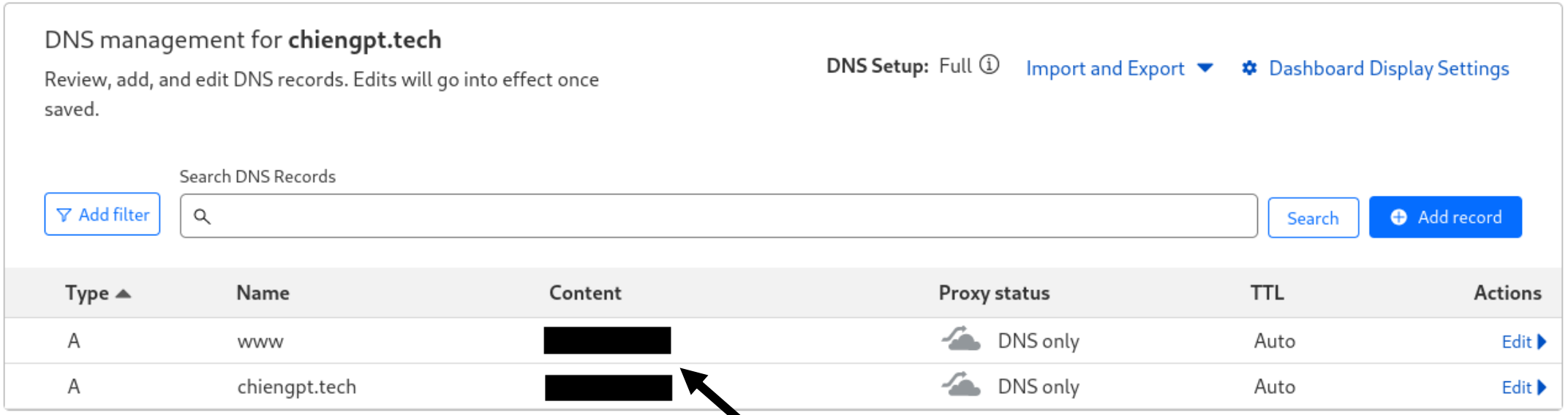
**`chiengpt.tech`**


*Registrar*



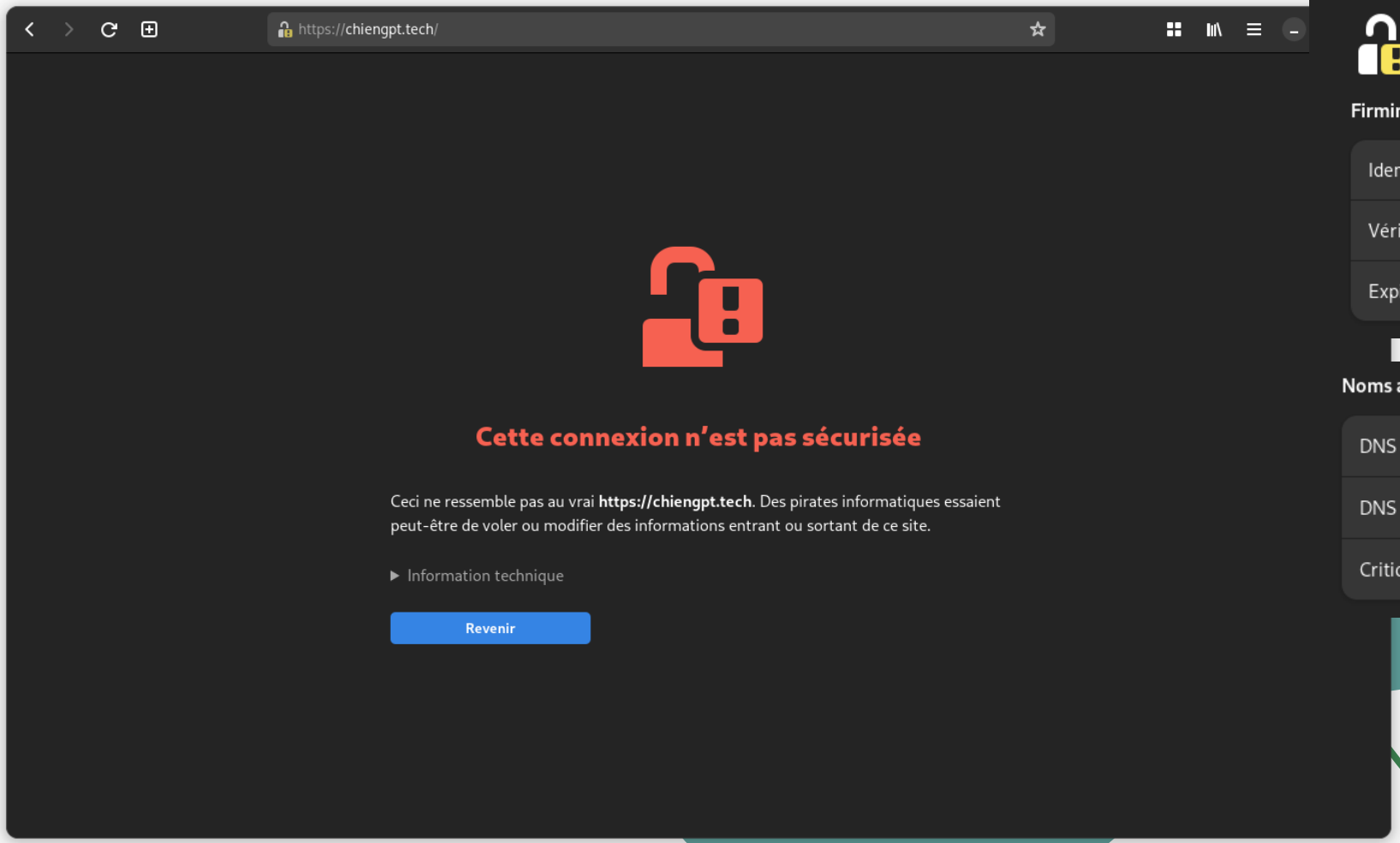

*Fournisseur des nameservers faisant autorité pour notre domaine*

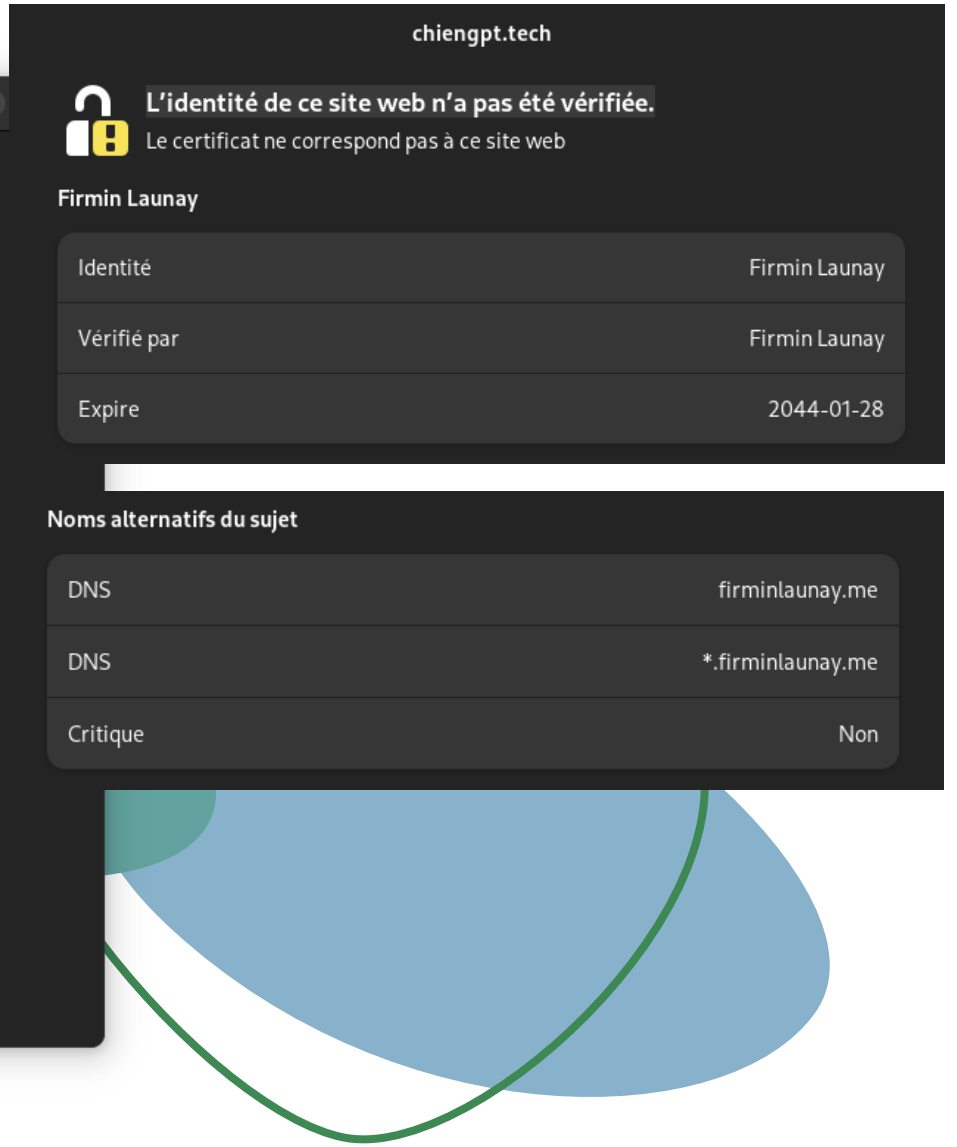
# Enregistrements A



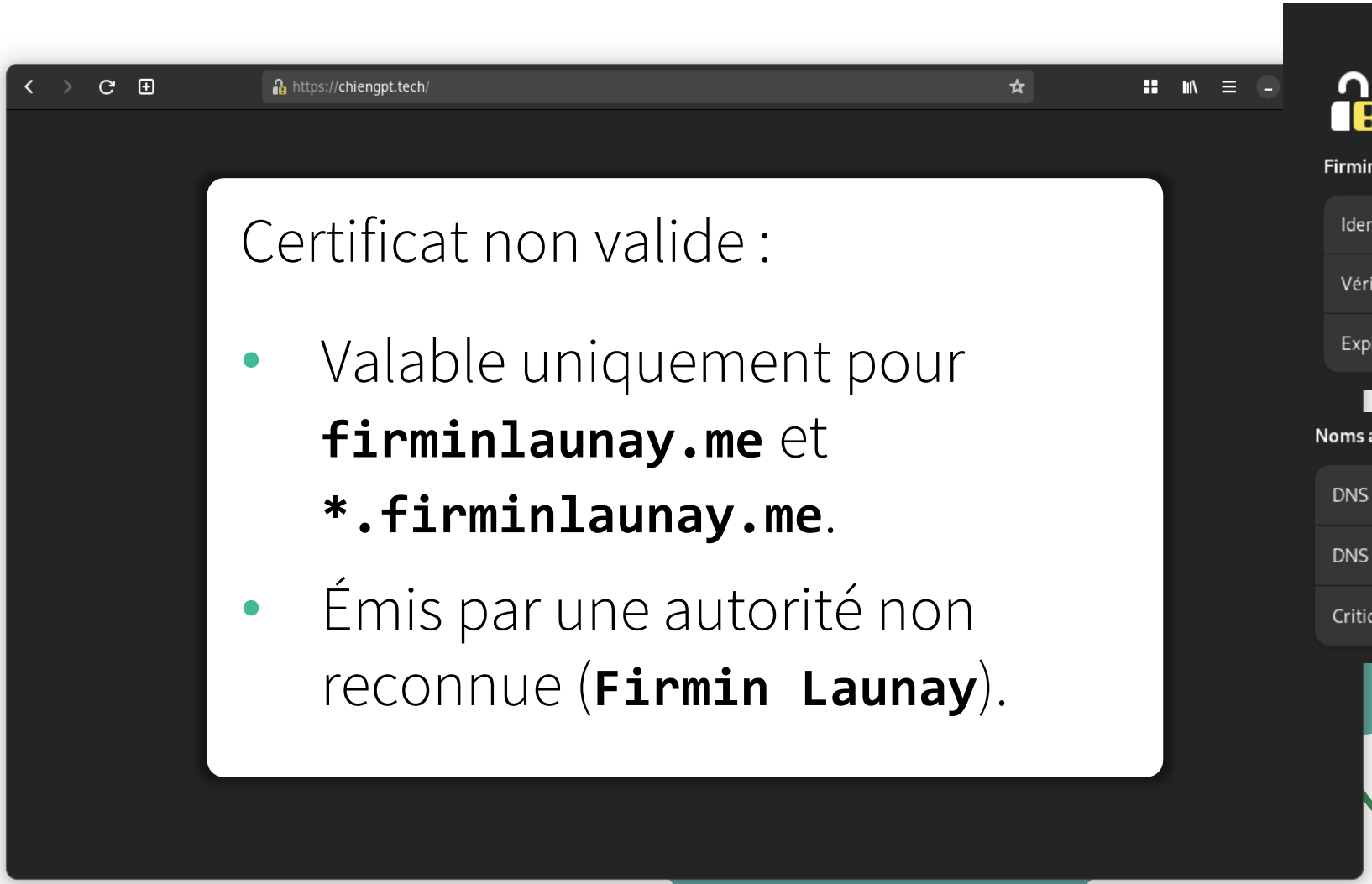

Adresses IP masquées par sécurité

# Erreur de certificat SSL



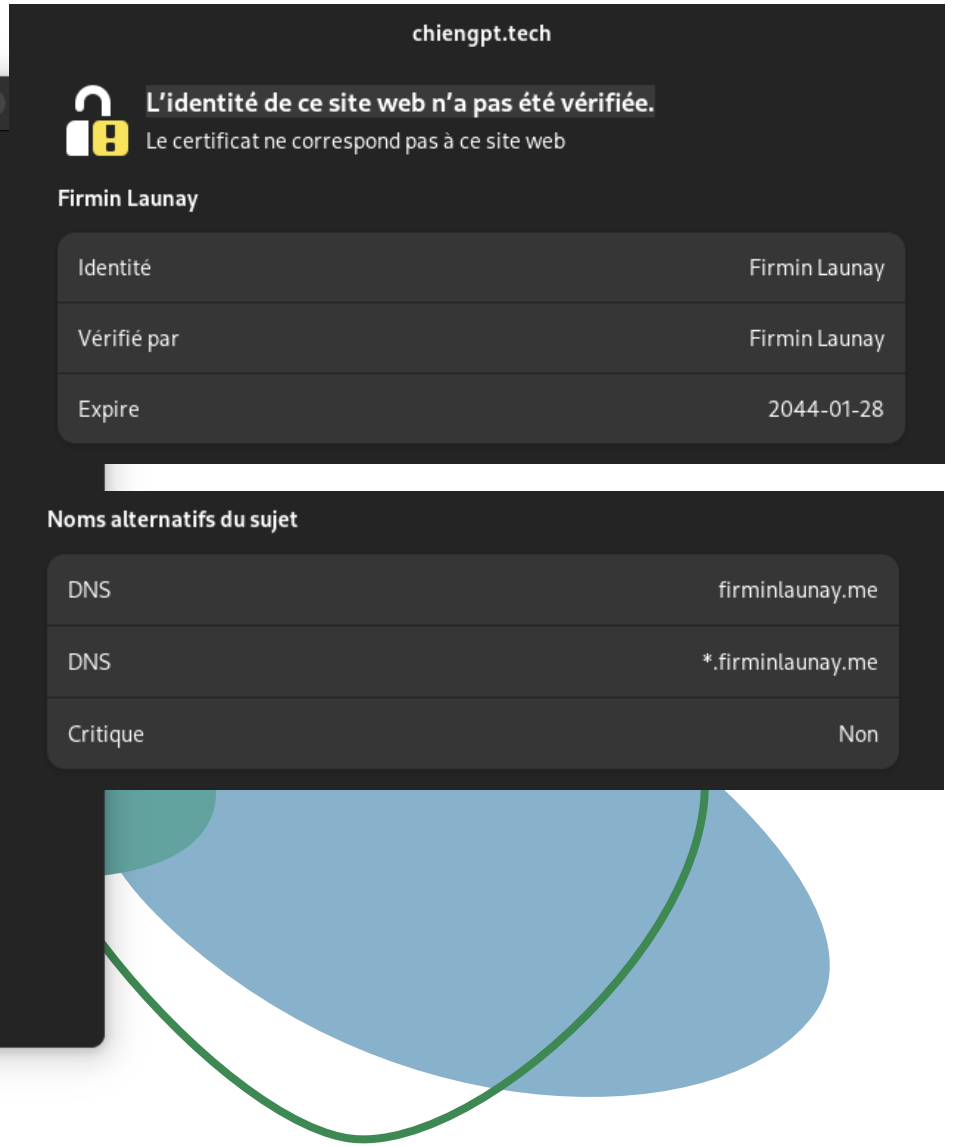



# Erreur de certificat SSL




Certificat non valide :

- Valable uniquement pour **`firminlaunay.me`** et **`*.firminlaunay.me`**.
- Émis par une autorité non reconnue (**`Firmin Launay`**).



# Mise en place d'un certificat SSL valide

## sur un autre serveur

SSH dans votre navigateur — IMPORTER UN FICHIER — TÉLÉCHARGER LE FICHIER

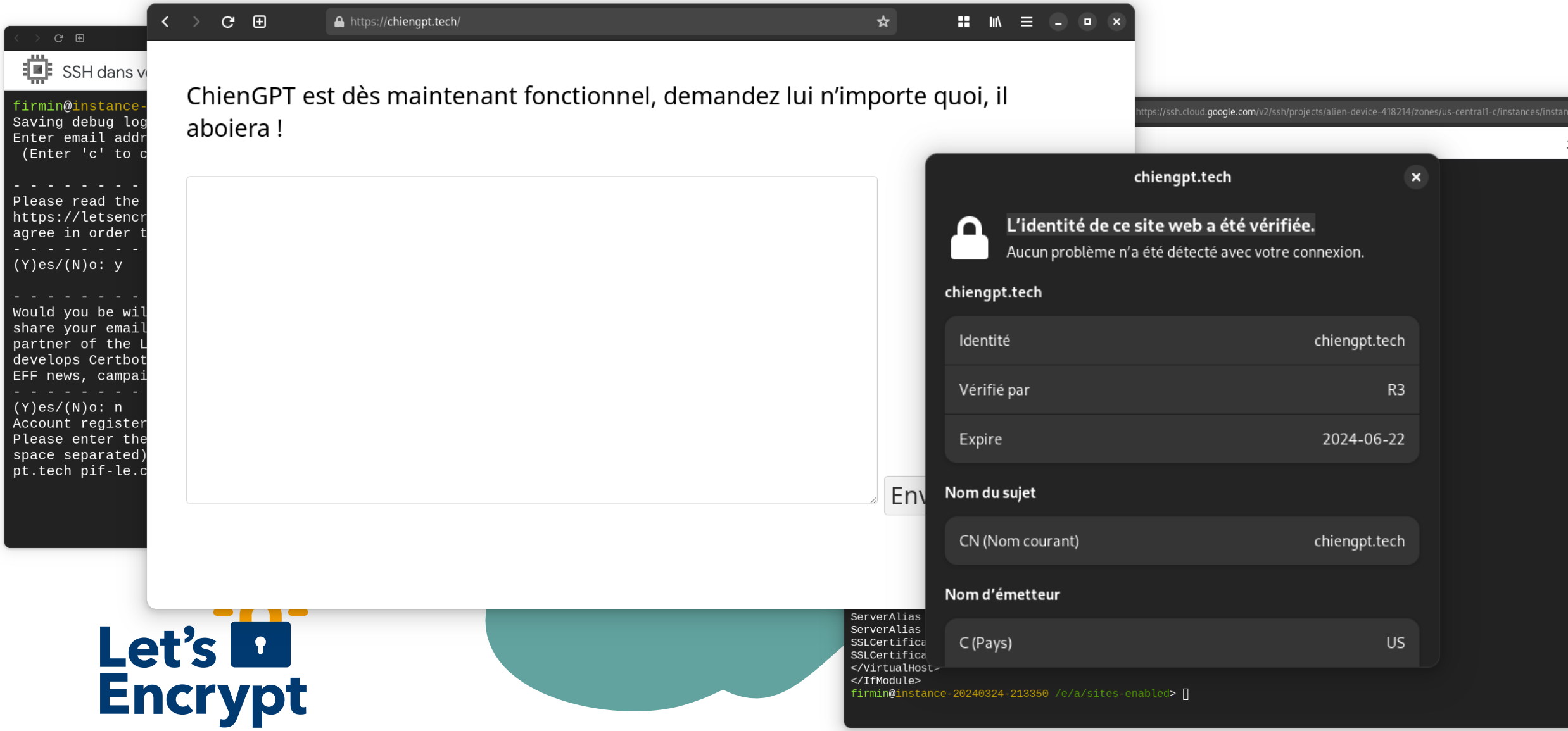
```
firmin@instance-20240324-213350 ~> sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): Firmin_Launay@etu.u-bourgogne.fr

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: n
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): chiengpt.tech www.chiengpt.tech les-chat-c-est-mieux-que-le
pt.tech pif-le.chiengpt.tech
```

SSH dans votre navigateur

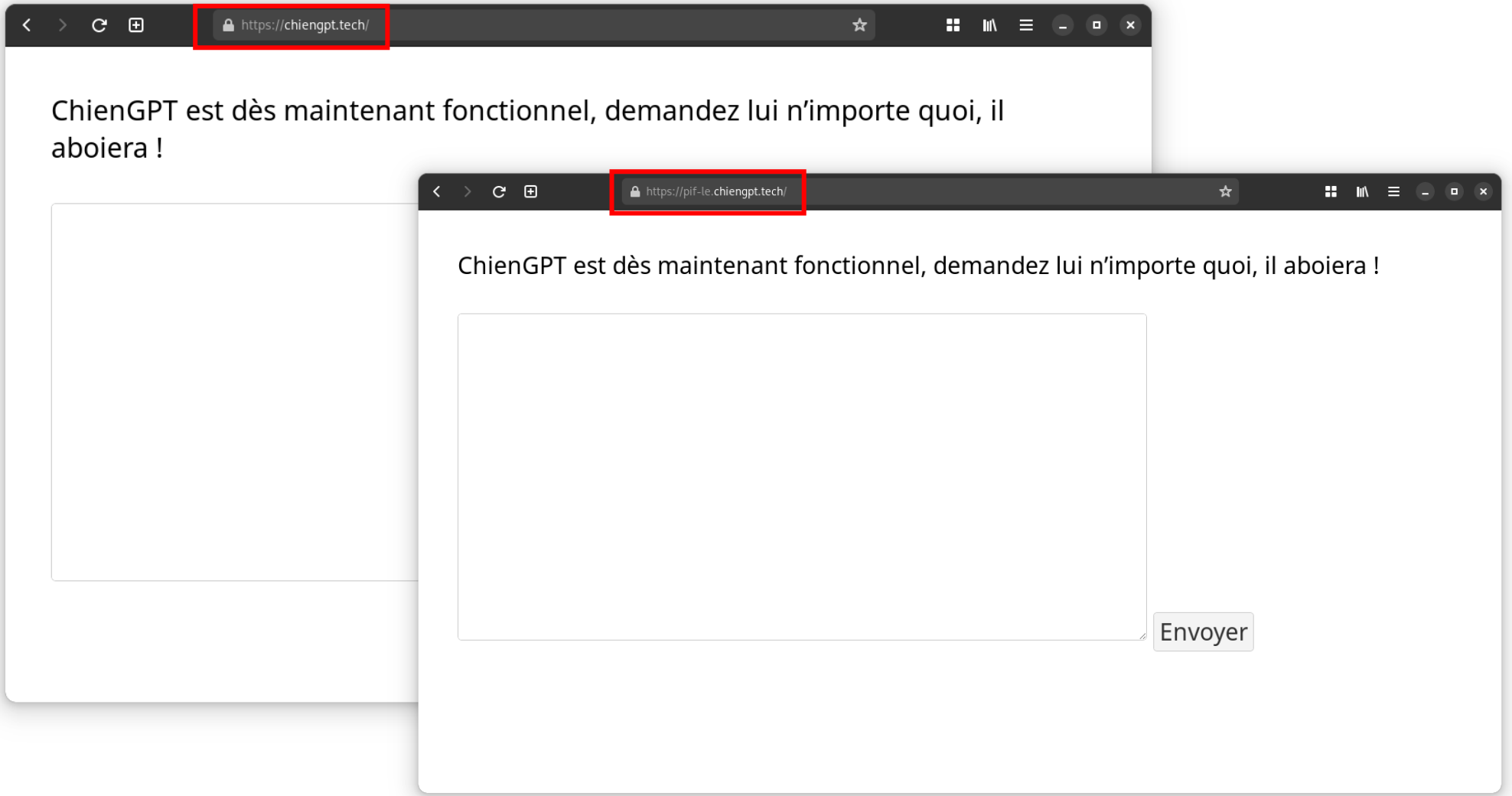
```
firmin@instance-20240324-213350 /e/a/sites-enabled> cat 000-default-le-ssl.conf
<IfModule mod_ssl.c>
<VirtualHost *:443>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf


ServerName chiengpt.tech
Include /etc/letsencrypt/options-ssl-apache.conf
ServerAlias www.chiengpt.tech
ServerAlias les-chat-c-est-mieux-que-les.chiengpt.tech
ServerAlias pif-le.chiengpt.tech
SSLCertificateFile /etc/letsencrypt/live/chiengpt.tech/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/chiengpt.tech/privkey.pem
</VirtualHost>
</IfModule>
firmin@instance-20240324-213350 /e/a/sites-enabled>
```

Let's Encrypt

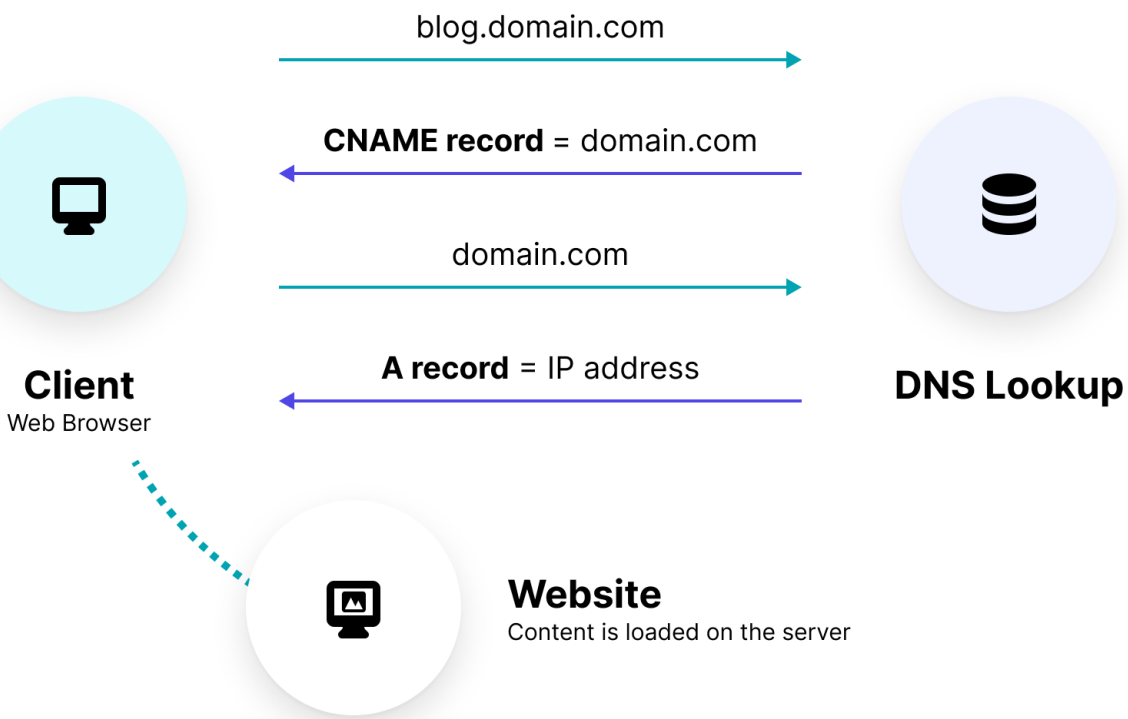
# Mise en place d'un certificat SSL valide



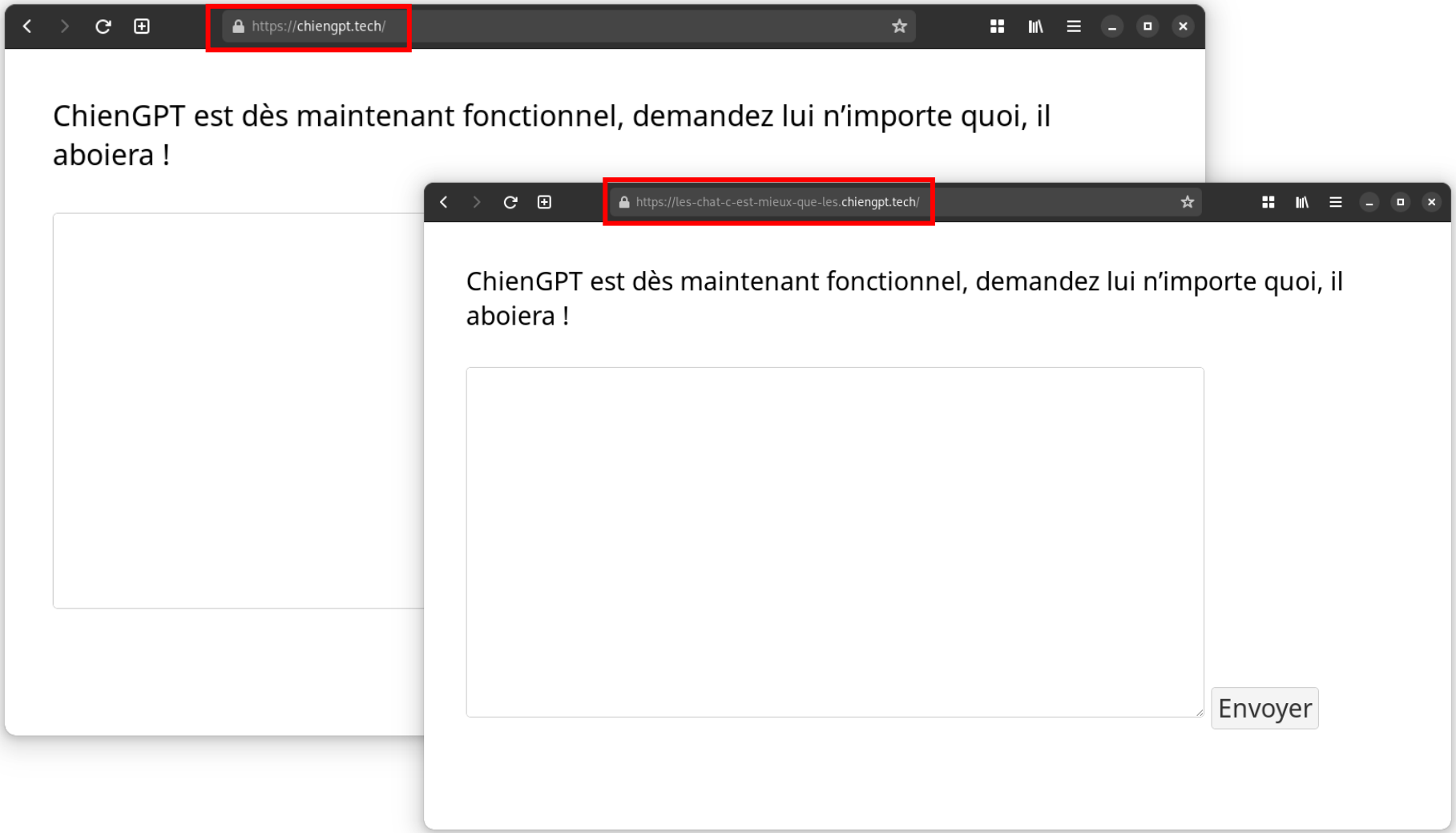
# Enregistrement AAAA



# Enregistrement CNAME



# Enregistrement CNAME



# Enregistrements MX & TXT

ImprovMX

chiengpt.tech DELETE

Email forwarding needs setup CHECK AGAIN

Aliases | DNS Settings | SMTP Credentials | Logs | Custom settings | STEP-BY-STEP | SUMMARY

No entries were found for the request.

**MX entries**

MX records are needed in order for ImprovMX to receive your emails and forward them. An MX record tells sending servers where to send the email.

We haven't found any MX records for your domain.

| | TYPE | HOSTNAME | PRIORITY | VALUE |
|---|---|---|---|---|
| ✗ | MX | chiengpt.tech. | 10 | mx1.improvmx.com. |
| ✗ | MX | chiengpt.tech. | 20 | mx2.improvmx.com. |

| | | | | | |
|---|---|---|---|---|---|
| MX | chiengpt.tech | mx2.improvmx.com | 20 DNS only | Auto | Edit |
| MX | chiengpt.tech | mx1.improvmx.com | 10 DNS only | Auto | Edit |
| TXT | chiengpt.tech | v=spf1 include:spf.improvmx.com ~all | DNS only | Auto | Edit |

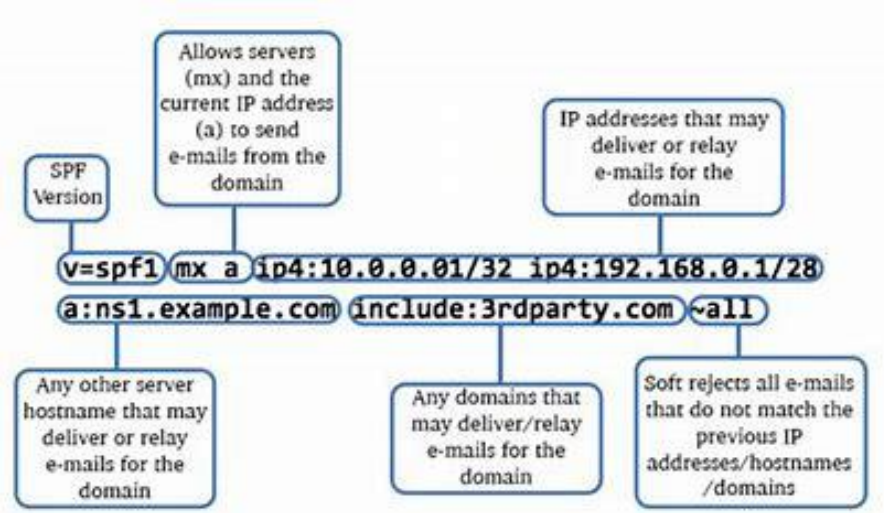
**SPF records**

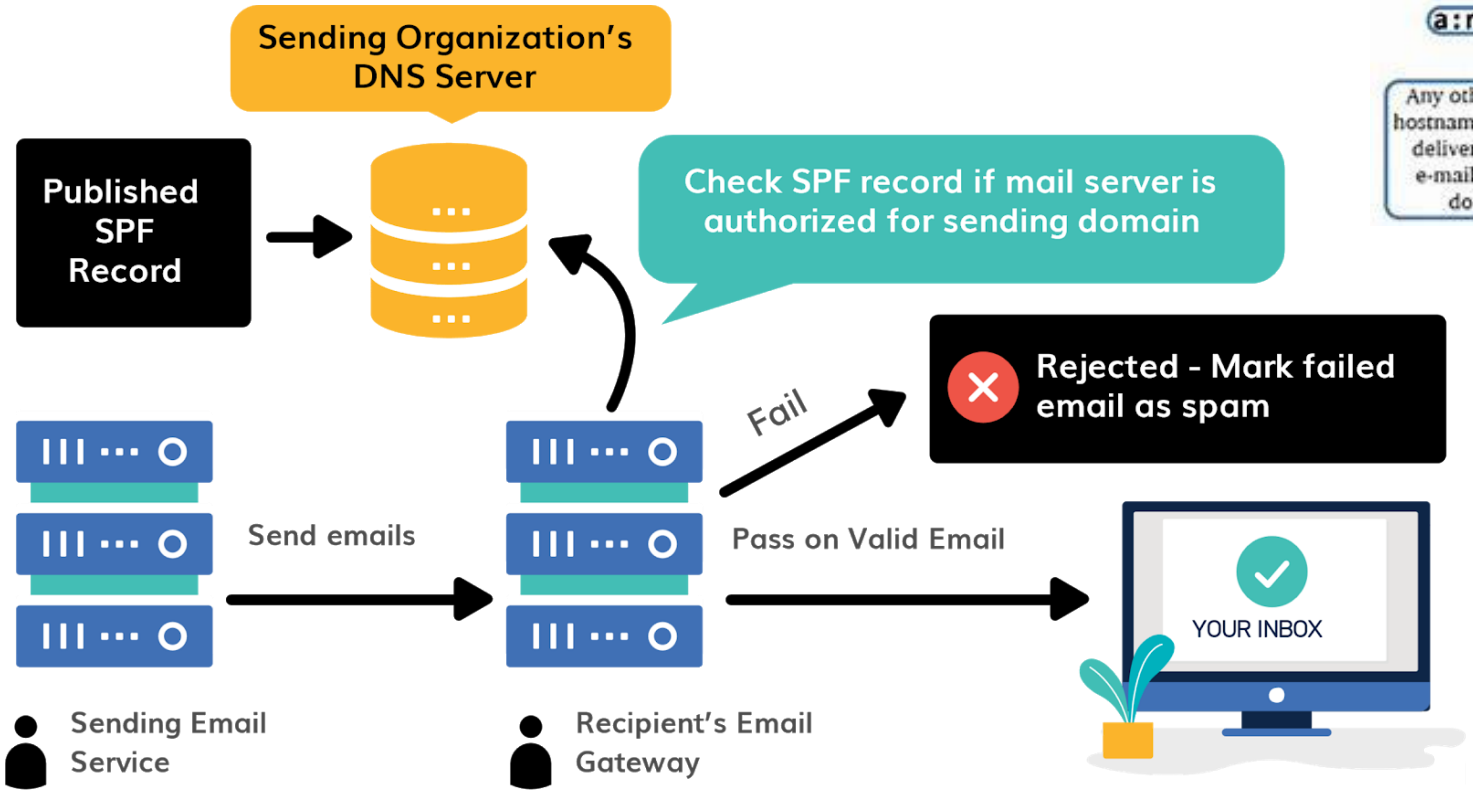
The purpose of SPF rec

Your SPF records is currently set to ***Nothing***

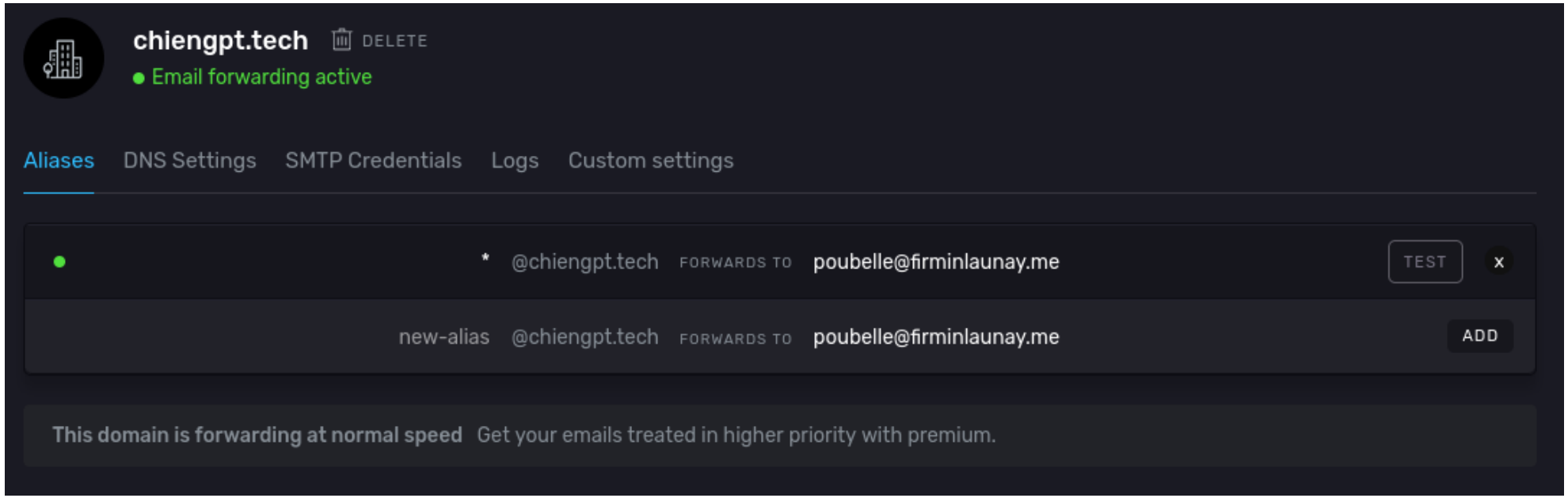
| | TYPE | HOSTNAME | RECOMMENDED VALUE |
|---|---|---|---|
| ✗ | TXT | chiengpt.tech. | v=spf1 include:spf.improvmx.com ~all |

# SPF

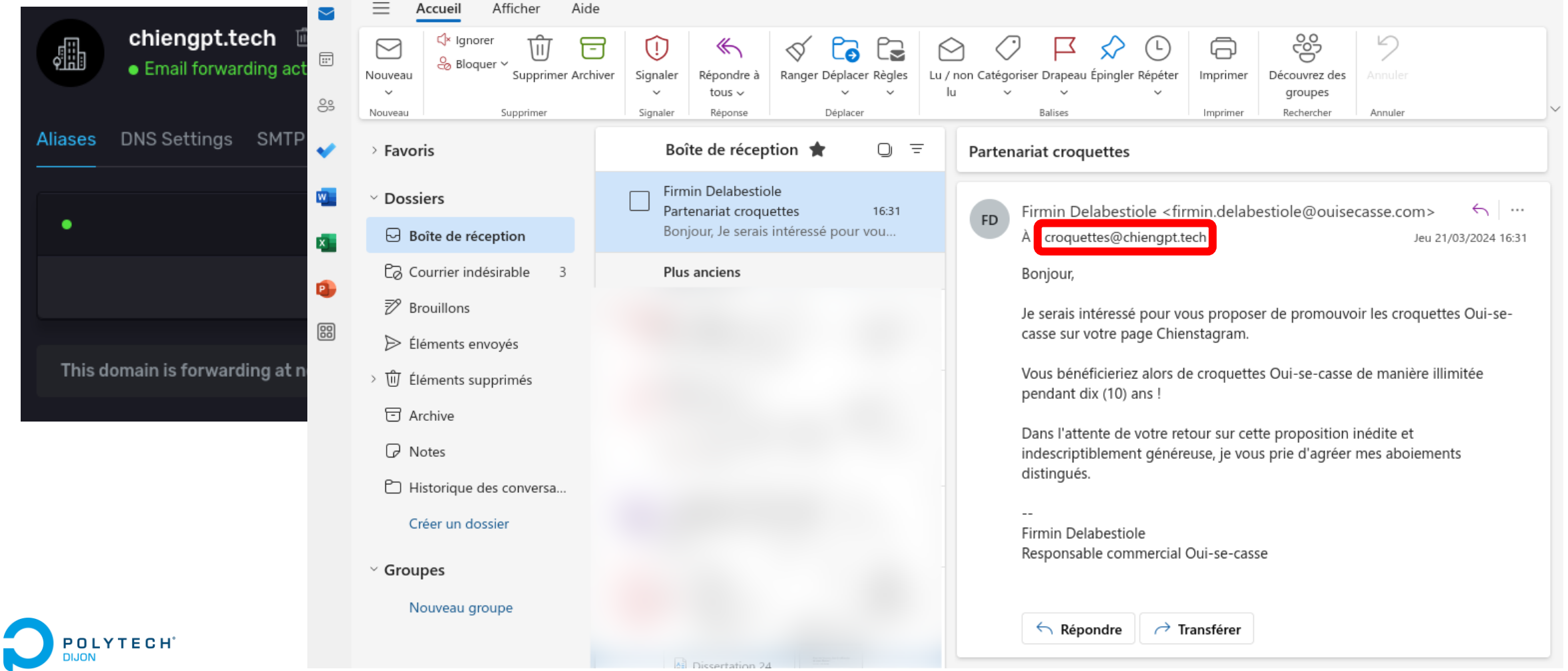

SPF Version
Allows servers (mx) and the current IP address (a) to send e-mails from the domain
IP addresses that may deliver or relay e-mails for the domain
v=spf1 mx a ip4:10.0.0.01/32 ip4:192.168.0.1/28
a:ns1.example.com include:3rdparty.com ~all
Any other server hostname that may deliver or relay e-mails for the domain
Any domains that may deliver/relay e-mails for the domain
Soft rejects all e-mails that do not match the previous IP addresses/hostnames /domains


Sending Organization's DNS Server
Published SPF Record
Check SPF record if mail server is authorized for sending domain
Fail
Rejected - Mark failed email as spam
Send emails
Pass on Valid Email
YOUR INBOX
Sending Email Service
Recipient's Email Gateway

# Enregistrements MX & TXT



# Enregistrements MX & TXT



# Enregistrement LOC

| LOC | chiengpt.tech | 47 18 45.114 N 5 4 27.935 E 256m 1m 10… | DNS only |
|---|---|---|---|

Type: LOC

Name (required): chiengpt.tech

Use @ for root

TTL: Auto

**Set latitude**

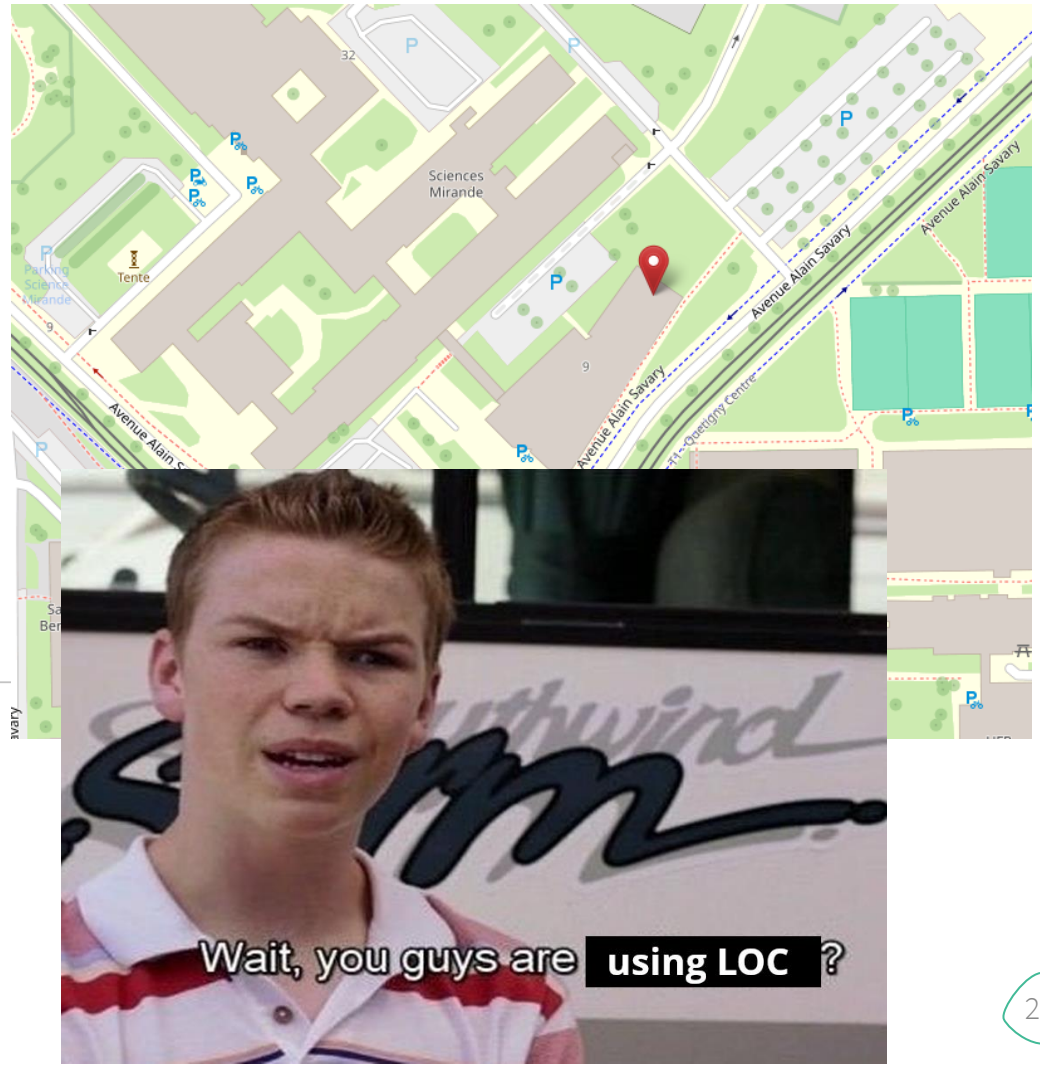
| Degrees (required) | Minutes (required) | Seconds (required) |
|---|---|---|
| 47 | 18 | 45,114 |

**Set longitude**

| Degrees (required) | Minutes (required) | Seconds (required) |
|---|---|---|
| 5 | 4 | 27,935 |

**Precision (in meters)**

| Horizontal (required) | Vertical (required) | Altitude (required) |
|---|---|---|
| 10 | 10 | 256 |



https://blog.cloudflare.com/the-weird-and-wonderful-world-of-dns-loc-records

CLOUDFLARE The Cloudflare Blog

Subscribe to receive notifications of new posts:

Email Address Subscribe

All Posts Product News Speed & Reliability Security Zero Trust Developers AI Policy Partners Life at Cloudflare

# The weird and wonderful world of DNS LOC records

04/01/2014

John Graham-Cumming

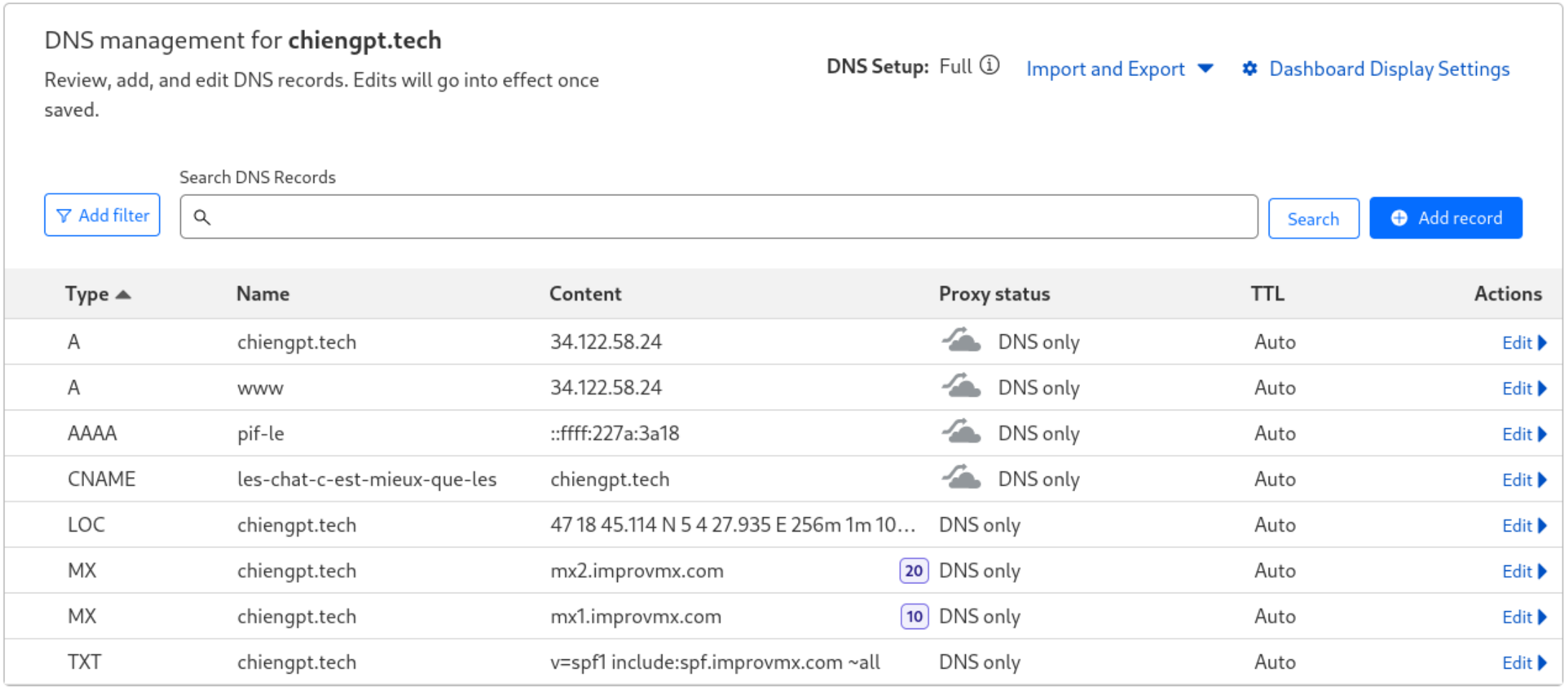
5 min read

A cornerstone of CloudFlare's infrastructure is our ability to serve DNS requests quickly and handle DNS attacks. To do both those things we wrote our own authoritative DNS server called RRDNS in Go. Because of it we've been able to fight off DNS attacks, and be consistenly one of the fastest DNS providers on the web.

Implementing an authoritative DNS server is a large task. That's in part because DNS is a very old standard (RFC 1035 dates to 1987), in part because as DNS has developed it has grown into a more and more complex system, and in part because what's written in the RFCs and what happens in the real-world aren't always the same thing.

One little used type of DNS record is the LOC (or location). It allows you to specify a physical location. CloudFlare handles millions of DNS records; of those just 743 are LOCs. Nevertheless, it's possible to set up a LOC record in the CloudFlare DNS editor.

# Les enregistrements DNS de `chiengpt.tech`



DNS management for **chiengpt.tech**

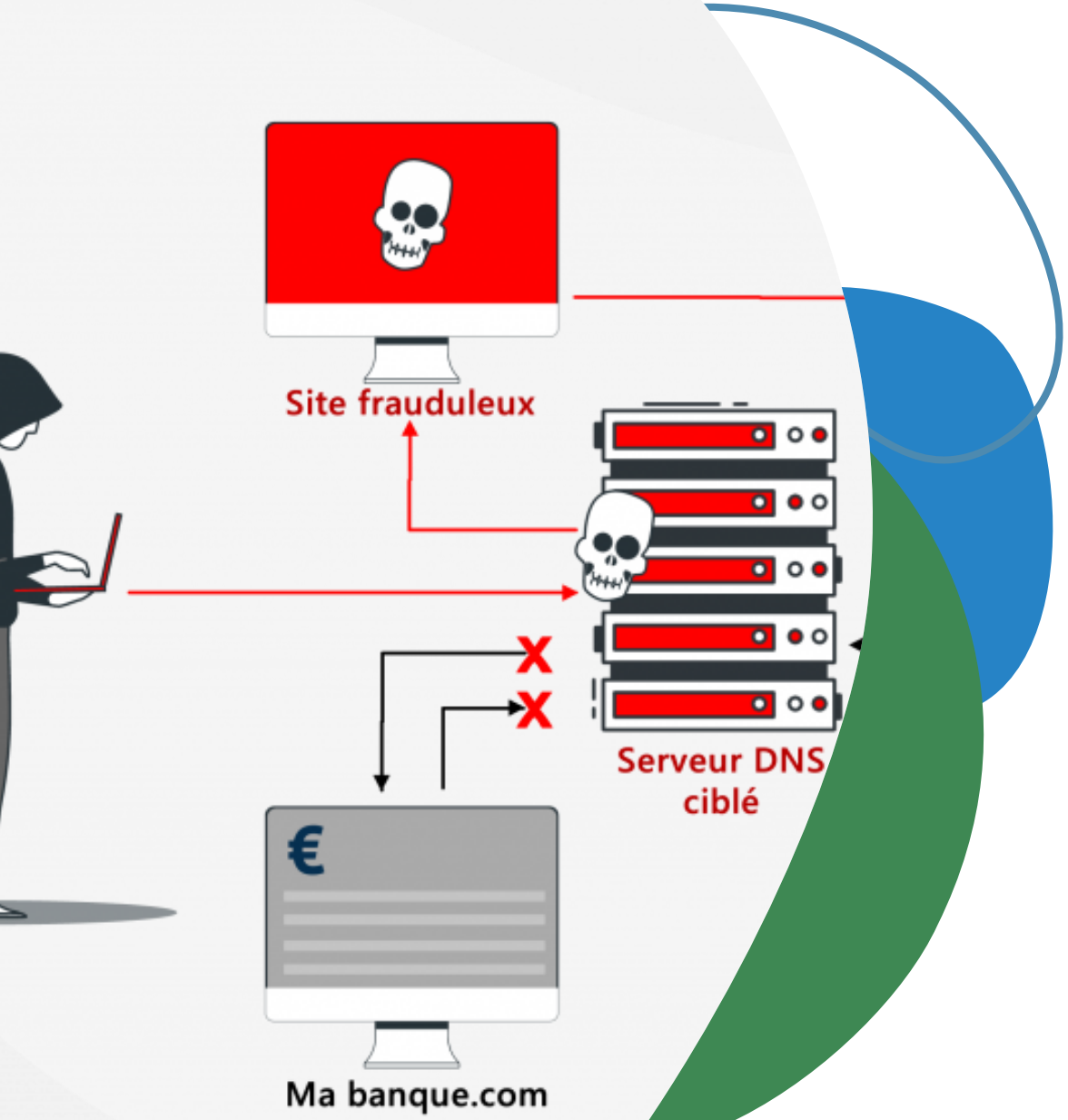
Review, add, and edit DNS records. Edits will go into effect once saved.

**DNS Setup:** Full ⓘ  Import and Export  Dashboard Display Settings

Search DNS Records

Add filter  Search  Add record

| Type ▲ | Name | Content | Proxy status | TTL | Actions |
|---|---|---|---|---|---|
| A | chiengpt.tech | 34.122.58.24 | DNS only | Auto | Edit |
| A | www | 34.122.58.24 | DNS only | Auto | Edit |
| AAAA | pif-le | ::ffff:227a:3a18 | DNS only | Auto | Edit |
| CNAME | les-chat-c-est-mieux-que-les | chiengpt.tech | DNS only | Auto | Edit |
| LOC | chiengpt.tech | 47 18 45.114 N 5 4 27.935 E 256m 1m 10… | DNS only | Auto | Edit |
| MX | chiengpt.tech | mx2.improvmx.com 20 | DNS only | Auto | Edit |
| MX | chiengpt.tech | mx1.improvmx.com 10 | DNS only | Auto | Edit |
| TXT | chiengpt.tech | v=spf1 include:spf.improvmx.com ~all | DNS only | Auto | Edit |

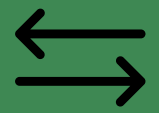



# Attaques sur les DNS

Présentation, tentative d'attaque

POLYTECH DIJON

# Attaques sur les DNS (T1071.004)

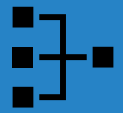


## DNS tunneling

Le DNS tunneling consiste à exploiter le protocole DNS pour encapsuler et transmettre de manière clandestine des données non autorisées à travers un réseau en contournant les mécanismes de sécurité traditionnels.

## DNS spoofing

Le DNS spoofing consiste à falsifier les réponses du serveur DNS afin de rediriger un utilisateur vers un site frauduleux pour voler des informations ou distribuer des malwares.



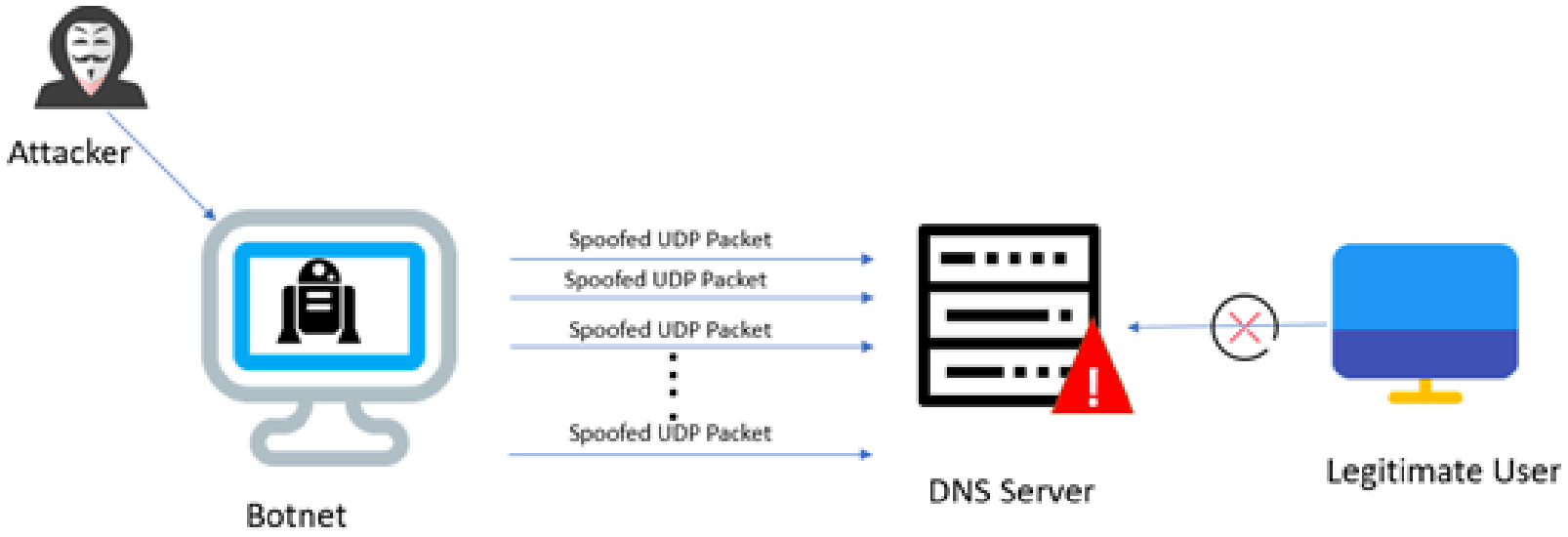
## (D)DoS

- (D)DoS
- Amplification DNS
- Domaines fantômes
- NXDOMAIN flooding

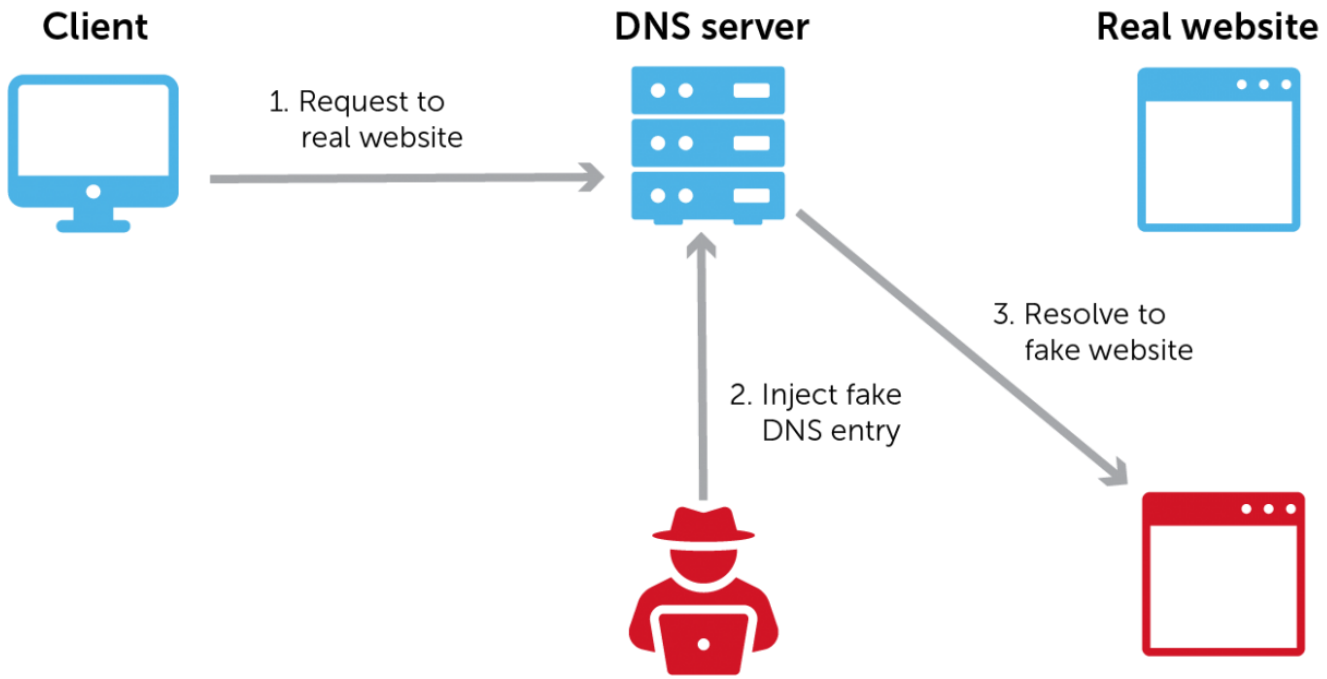
## DNS hijacking

Le DNS hijacking consiste à prendre le contrôle d'une session DNS pour rediriger les utilisateurs vers des sites frauduleux, souvent pour faire du phishing ou de la distribution de malware.

# DDoS (DNS amplification)

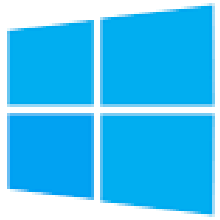


# DNS spoofing

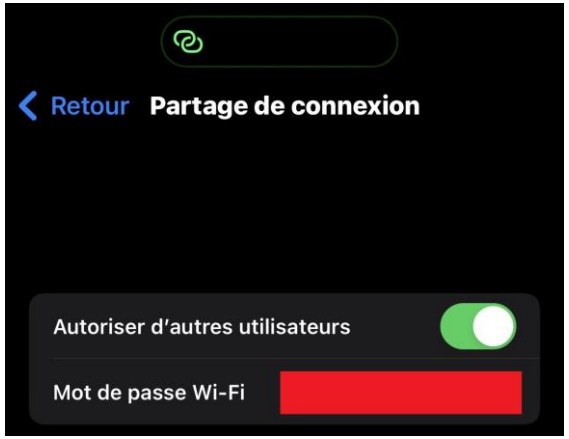


# DNS spoofing (démo)

Bettercap, framework de pentest pour les réseaux écrit en Go



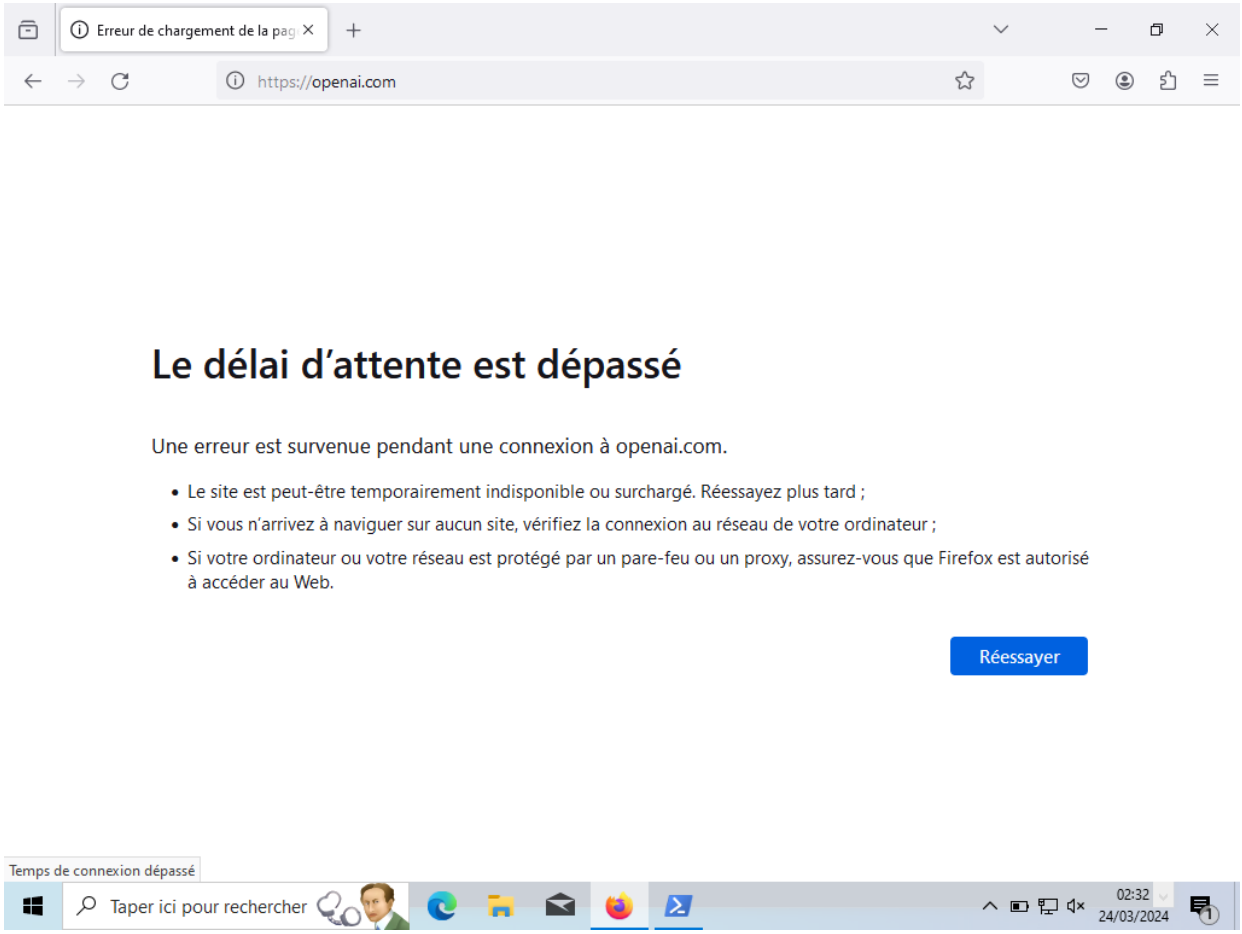

Machine victime

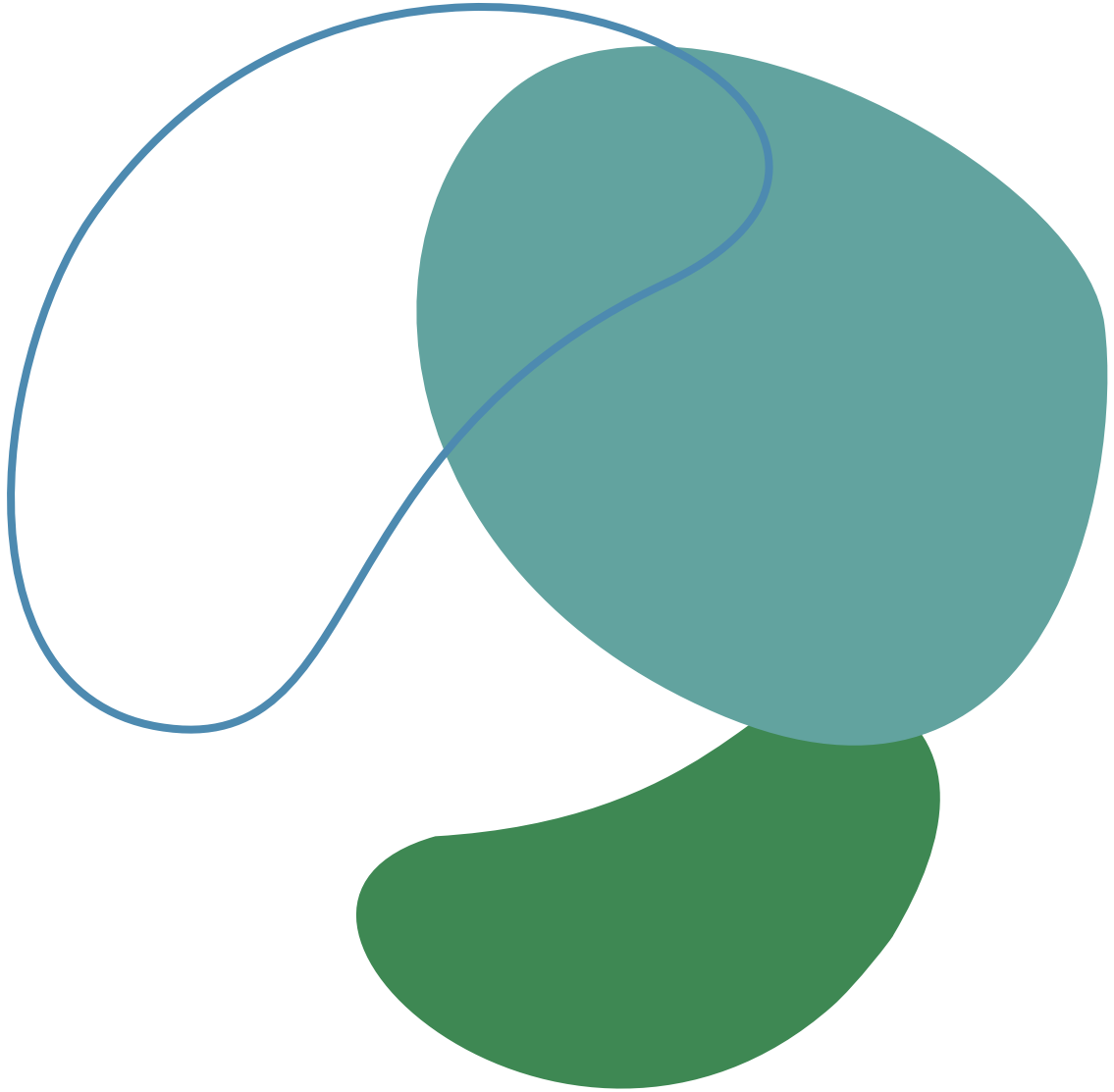



Le réseau sera mon partage de connexion

# DNS spoofing (démo)

# DNS spoofing (démo)



# Merci de votre attention !

Paul DUCOLOMB
Firmin LAUNAY
Théophile REY

POLYTECH DIJON