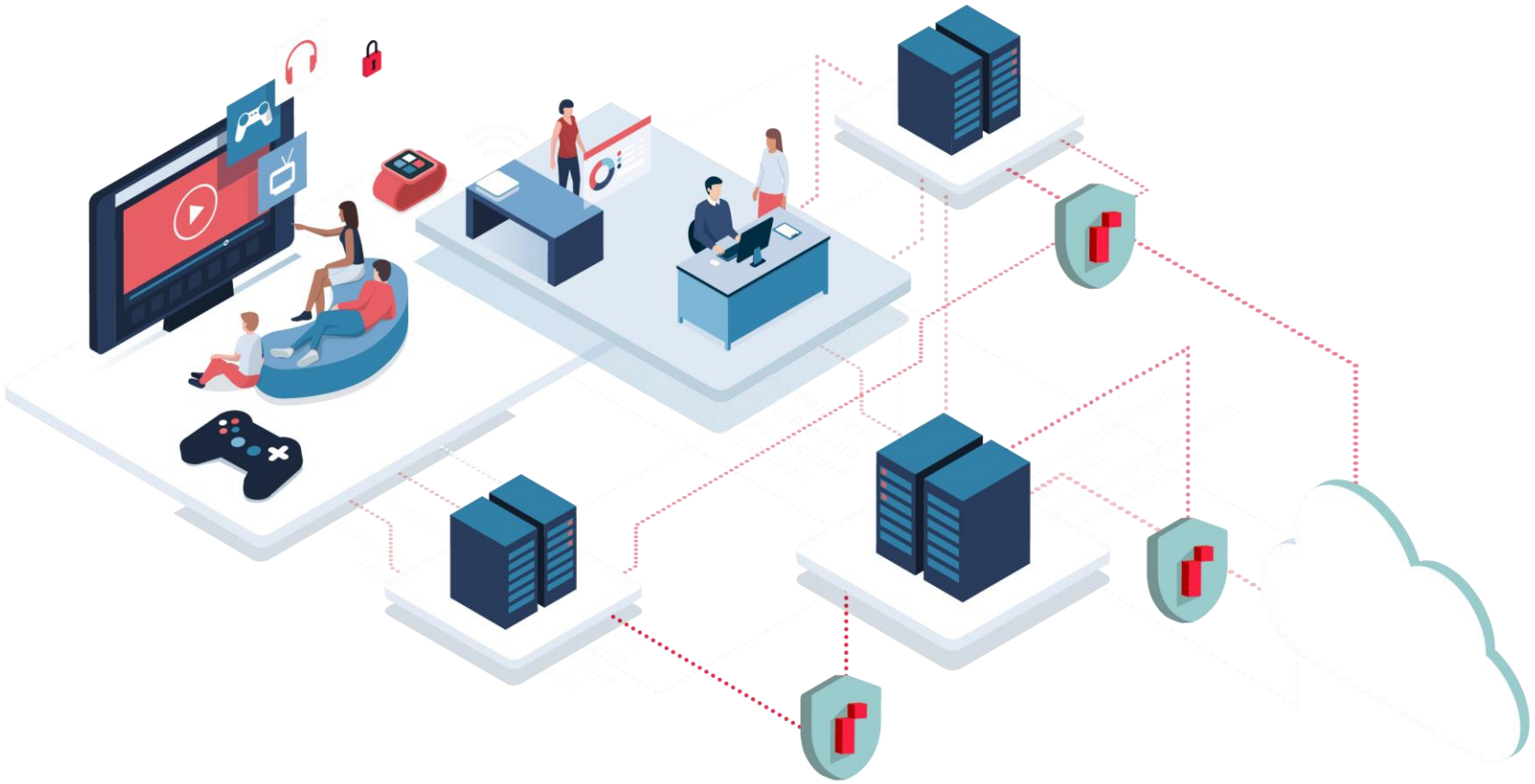
alternativ.net

by

alternativ



alternativ.net

Let's be clear in one second

	.NET	VPN	Tor	I2P net.	JonDonym	Nym
Delivers privacy	✓	✓	✓	✓	✓	✓
No trusted third party	✓	x	x	x	x	x
Immune to basic traffic basic analysis	✓	x	✓	✓	x	?
Immune to AI-based traffic analysis	✓	x	x	x	x	?
Node integrity guarantees	✓	x	x	x	x	x
Low latency dependency	✓	x	x	x	x	x
Acces control	✓	✓	x	x	x	✓
Delivers security	✓	✓	x	x	x	x
imune to MITM	✓	x	x	x	x	x
Additional features						
Routes	*Dynamic*	*Static*	*Random*	*Random*	*Static*	*Random*
Active counter-measures	✓	x	x	x	x	✓
Hide surface attack	✓	x	x	x	x	x
Mass surveillance proof	✓	x	x	x	x	x
Easy to use	✓	x	x	x	x	✓
Agility	✓	x	x	x	x	x
QoS	✓	✓	x	x	✓	✓

altrnativ.net

State of the art

SECURITY is **Confidentiality** and **integrity** of the content
"No one can see or alter what Alice is saying to Bob"

SECURITY excludes **PRIVACY**
and
PRIVACY excludes **SECURITY**

PRIVACY is Anonymity of the end-points
"No one can know Alice is talking to Bob"

Antagonistic properties today

⇩

(very) easy to track & crack!

Altrnativ.net combines both synergistically

altrnativ.net

altrnativ.net threat model vs. existing threat models

Existing Threat model

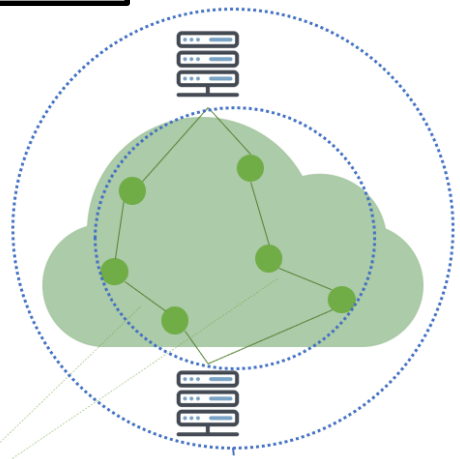
Security level = static figure A

Privacy level = f (users)

Altrnativ.net Threat model

Privacy level = static. fig B + g (users)

Sec. level = static fig. C + h (Privacy level)



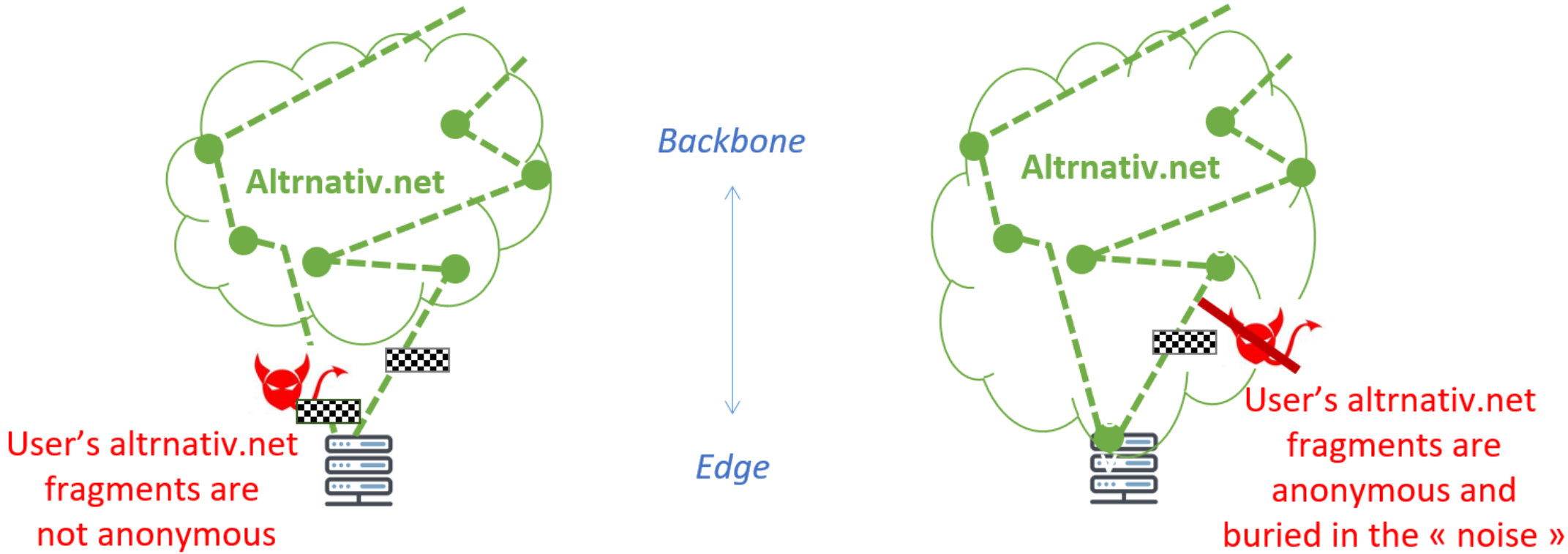
User route = distinct circuits going through Holo nodes

User chooses "area" covered by its route

Wider area = Increased anonymity & Enhanced security

altrnativ.net

CLIENTS and/or USERS benefit from contributing to the infrastructure



altrnativ.net

Additional advantages of altrnativ.net
Beyond-trust architecture

Privacy:
- No trusted-third party
- Much harder attack through traffic analysis

Security:
- No MITM
- Obfuscated surface attack
- Security outpost

Central management:
- Capacity to guarantee Privacy & Security levels (e.g. traffic injection)
- Capacity for user to modulate these levels
- Capacity to deploy remote attestation at central & user level
- Capacity to operate SoC

altrnativ.net

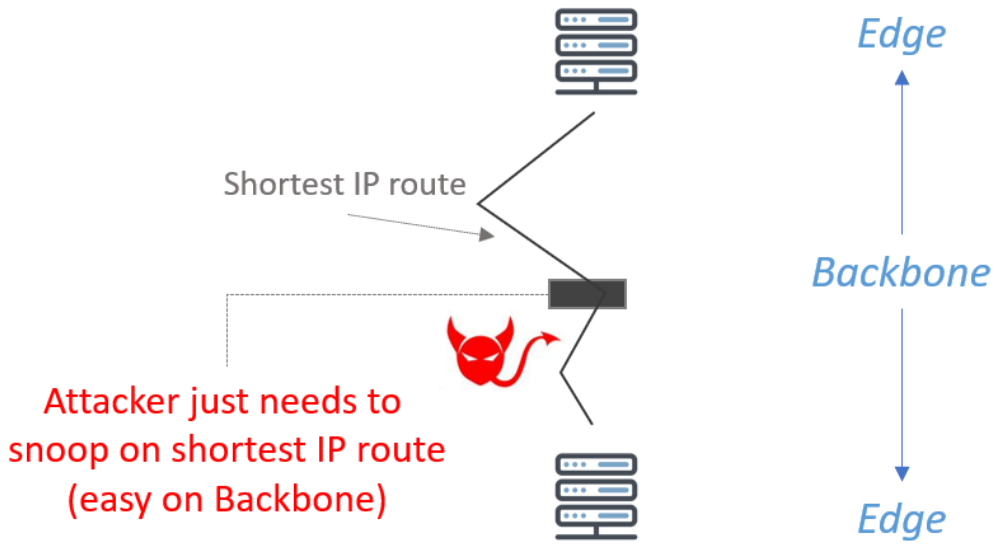
How altrnativ.net hampers mass-surveillance (and network threats)

Based on 2 patents

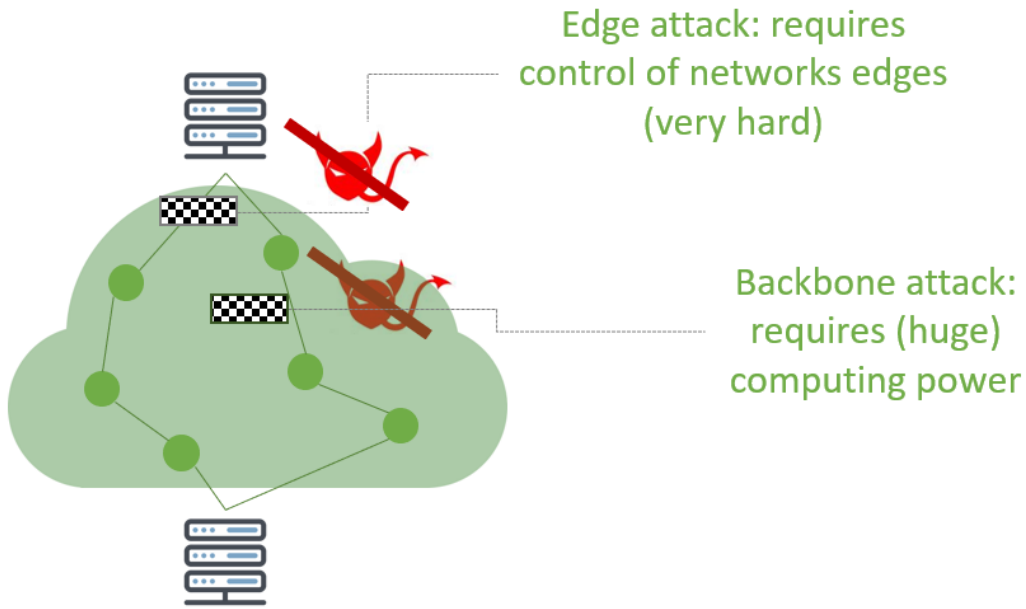
cea

FR1759452 "Dispositif et procédé d'anonymisation et de sécurité des données"

existing Threat model



altrnativ.net Threat model



IP packet has all data and is easily spoted

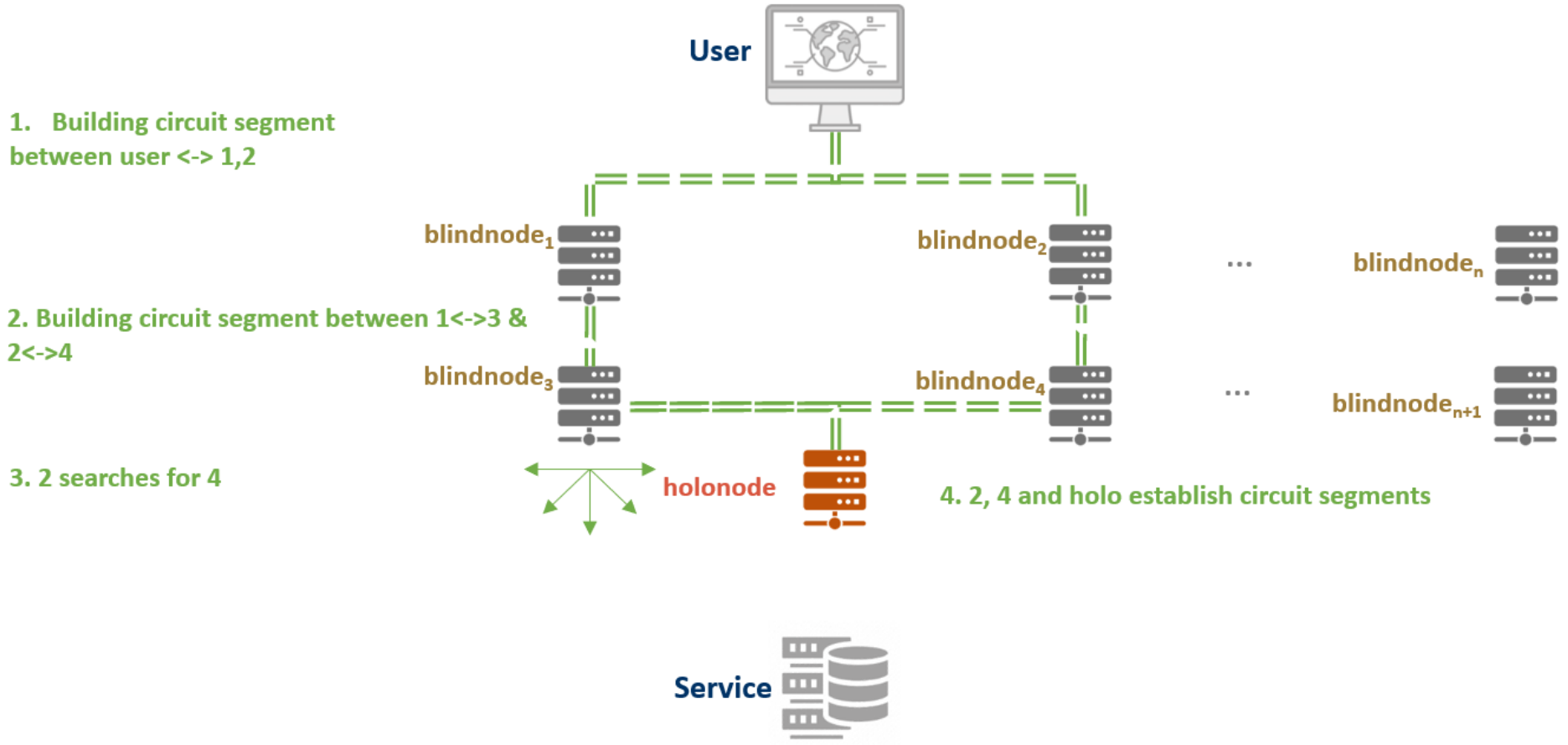
Altrnativ.net fragment is anonymous noise

=> +

altrnativ.net

altrnativ.net main protocol principles

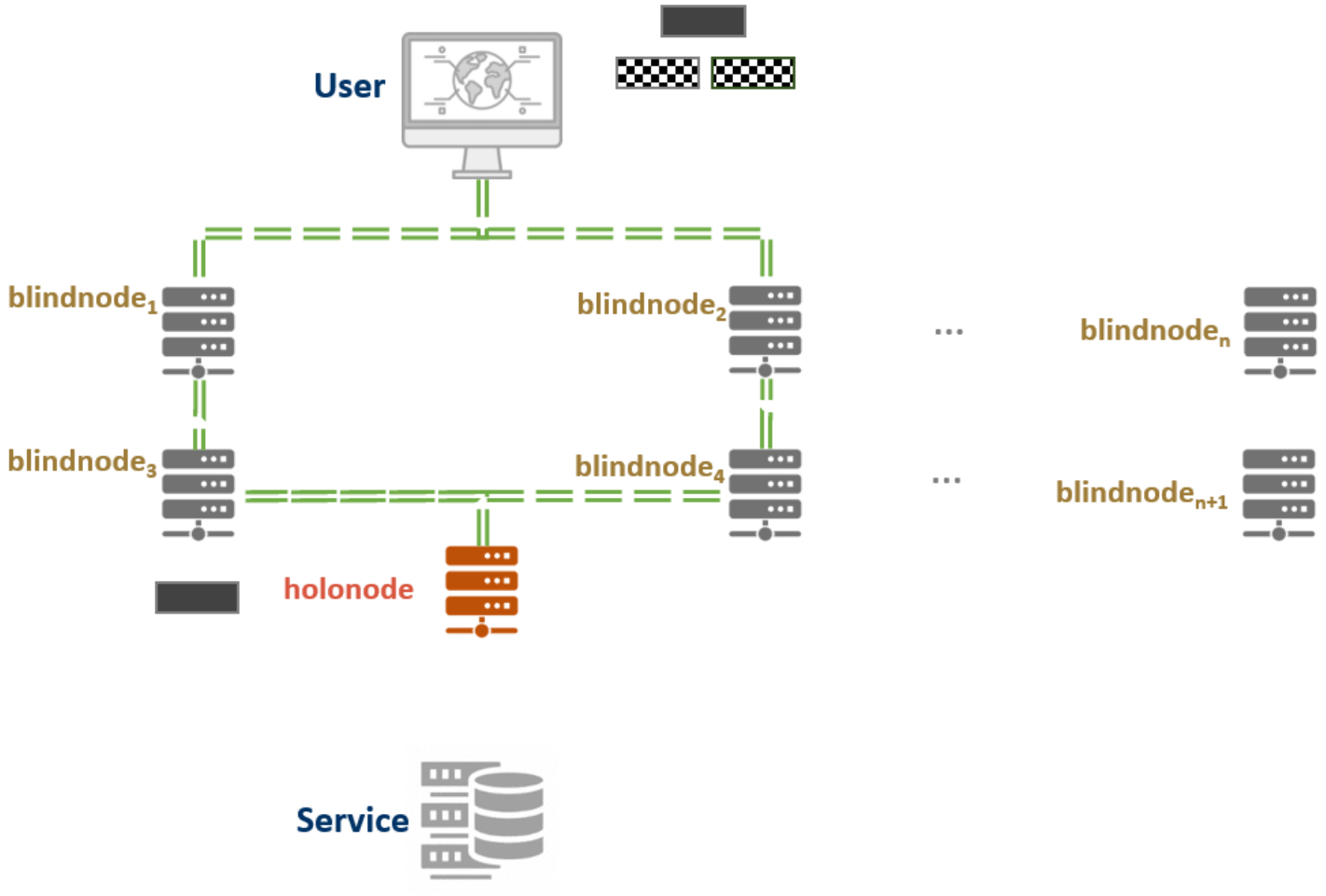
Step 1: building route



altrnativ.net

altrnativ.net main protocol principles

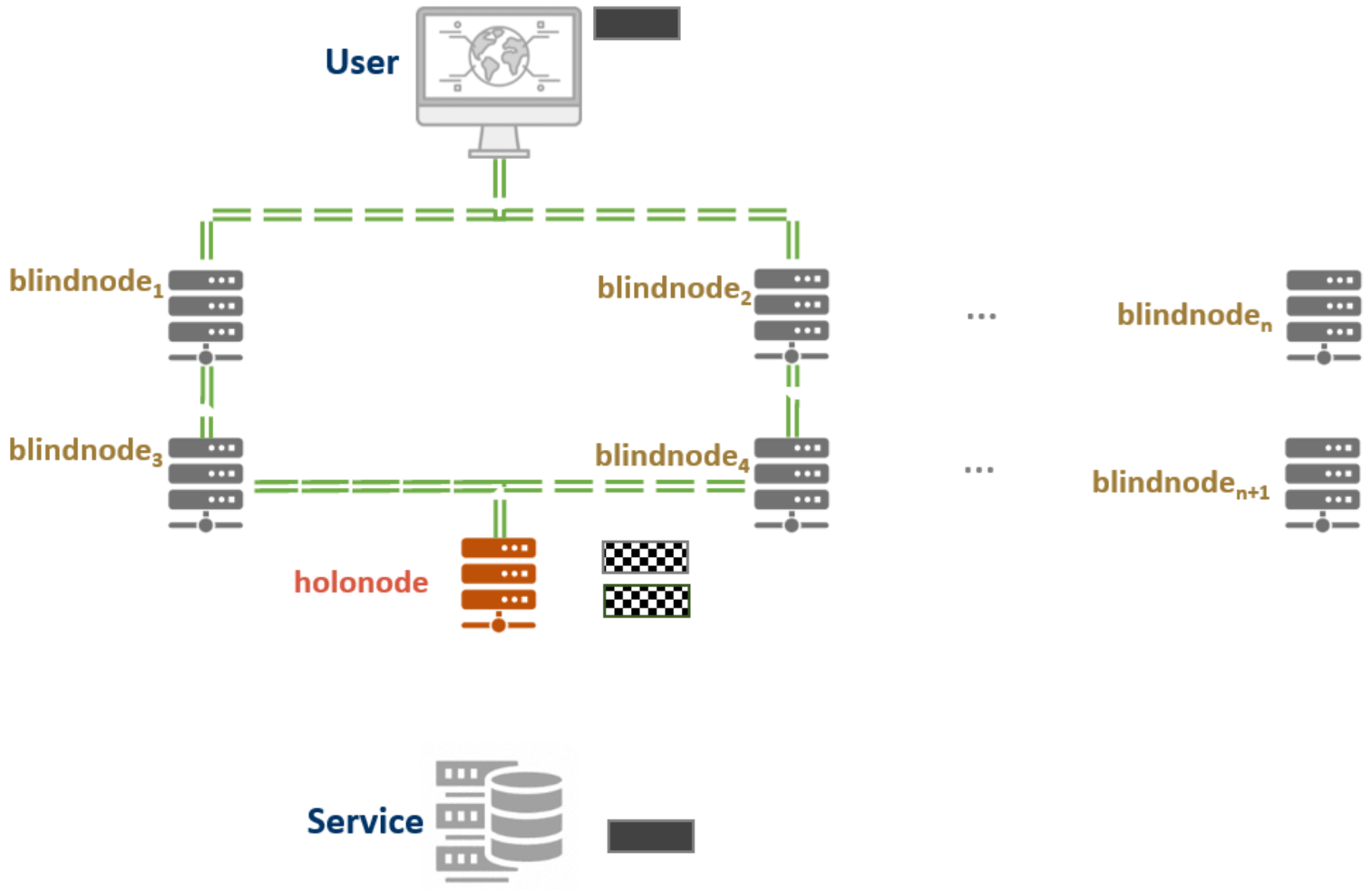
Step 2: sending packets



altrnativ.net

altrnativ.net main protocol principles

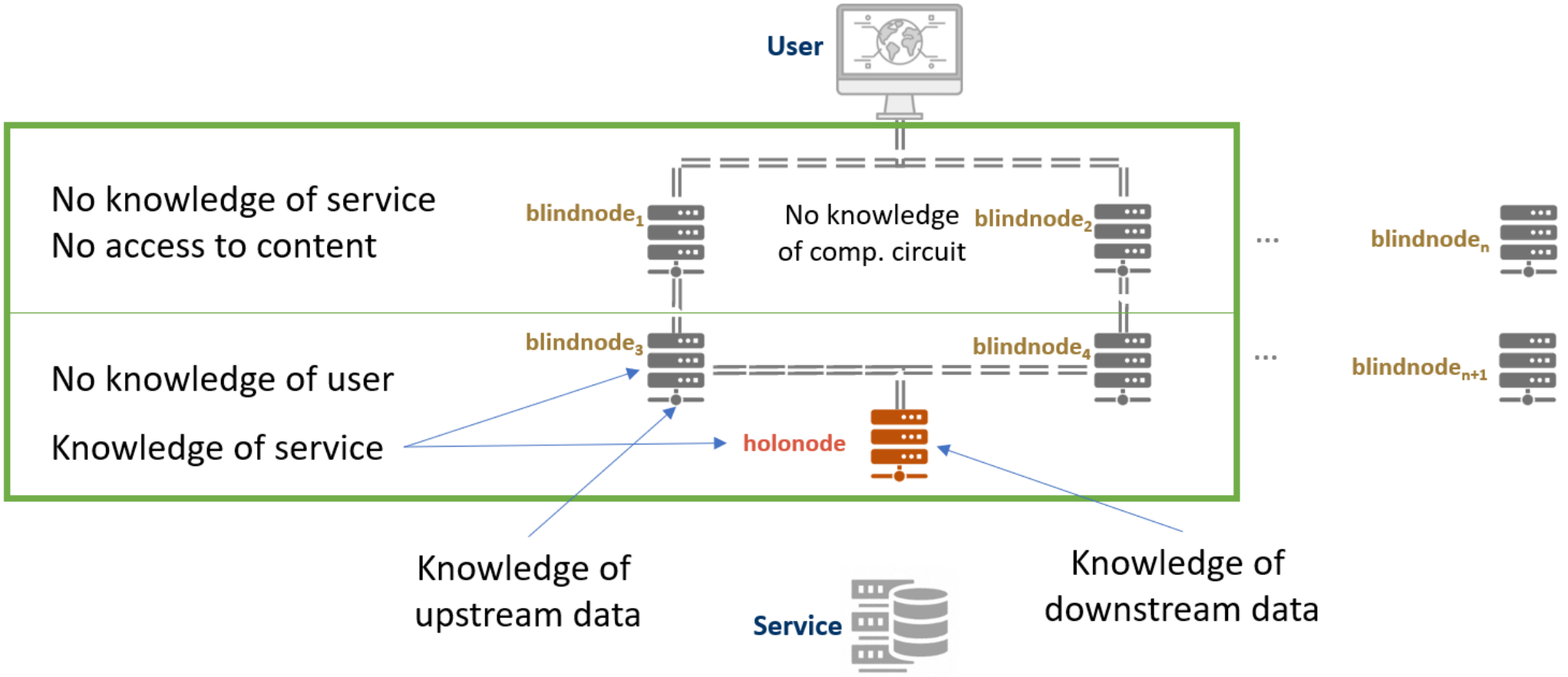
Step 3: receiving packets



altrnativ.net

altrnativ.net main protocol principles

Summary of properties



altrnativ.net

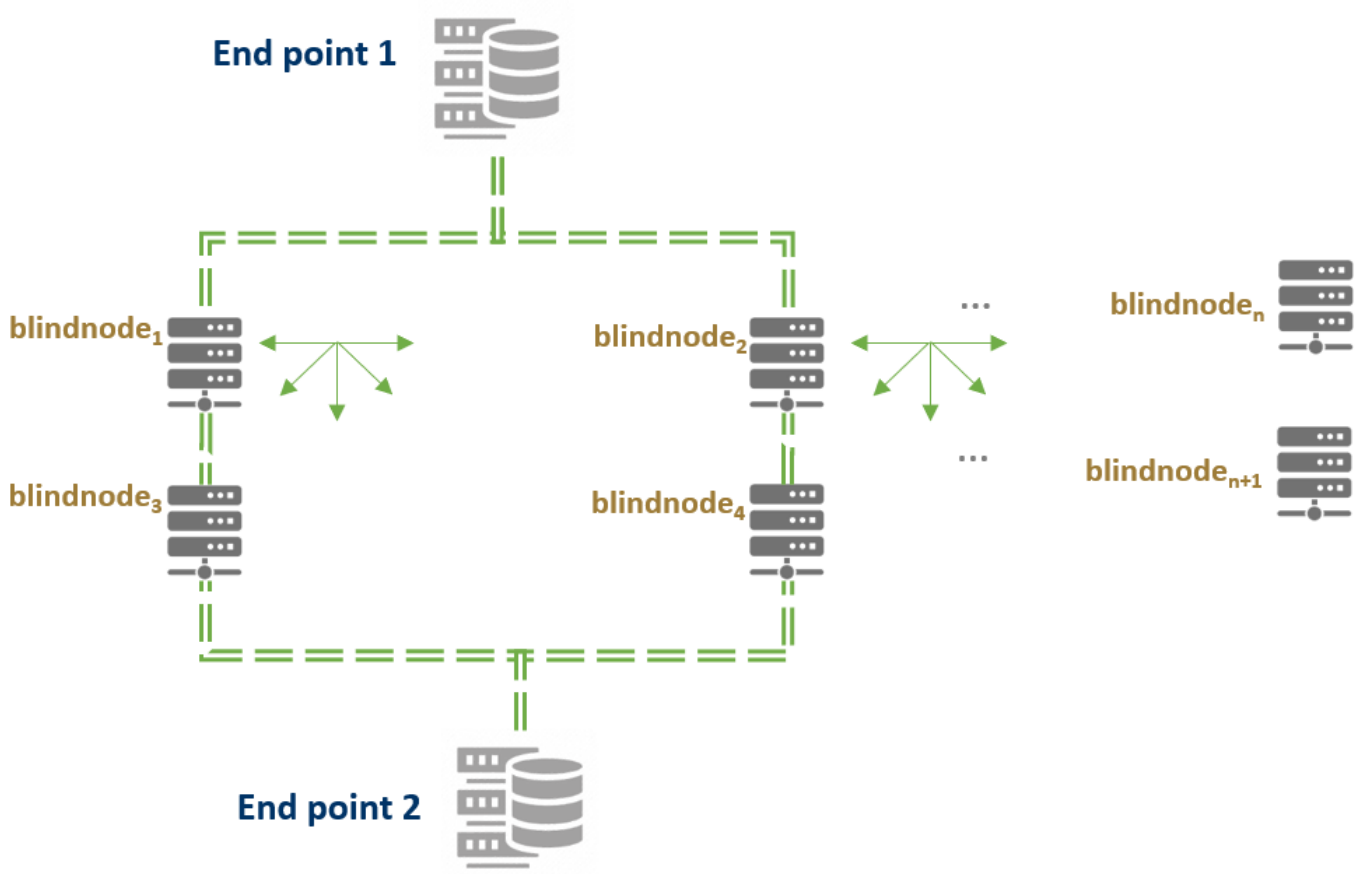
altrnativ.net main protocol principles

Security usage

1. Building circuit segments between EP1<->1,2 & EP2<->3,4

2. 1 & 3 search for 3 & 4

3. Connexions 1<->3 & 2<->4



alternativ.net

DNS OVER HTTPS .doh

Accroître la confidentialité et la sécurité des utilisateurs en empêchant les écoutes clandestines et la manipulation des données.

SITUATION

- Le serveur **DNS** (Domain Name System) est le service qui permet **d'associer à site web** (ou un ordinateur connecté ou un serveur) **une adresse IP**
- Le **DNS** associe un URL (ou adresse web) à une adresse IP (longue suite de chiffres), **comme un annuaire téléphonique** associe un numéro à un nom
- L' internaute qui va sur Twitter par exemple tape *www.twitter.com* (L'URL) sur le navigateur
- L'adresse **est lisible pour l'humain**, mais **illisible pour les ordinateurs**, qui ne comprennent que l'adresse IP
- Le navigateur contacte donc un **DNS pour traduire** l'URL en adresse IP à l'ordinateur
- La **connexion** à un site web passe donc en **deux temps** : l'adresse IP du site voulu est récupérée puis les paquets sont envoyés directement à cette adresse

PROBLÈMES

- Toutes les **requêtes DNS** d'un internaute sont lisibles ; elles ne sont **ni chiffrées, ni sécurisées**
- Les **informations** relatives à l'activité de l'internaute sont donc **faciles à récolter** et à **utiliser**
- La lisibilité des requêtes DNS peut entraîner des **fuites de données personnelles** ou le **tracking** des activités de l'internaute
- Les DNS utilisés par défaut sont ceux du **fournisseur d'accès** auquel l'appareil utilisé est connecté : ils peuvent se servir des informations transmises **à mauvais escient**, comme pour **diffuser de la publicité**

SOLUTION

- .DOH met en place un **mécanisme** qui permet de **sécuriser les requêtes DNS** en utilisant un protocole spécifique, le *DNS Queries over HTTPS*
- Le HTTPS **sécurise** la navigation sur **le web** en vérifiant la fiabilité des sites visités
- Le **DoH** est un protocole qui utilise HTTPS pour **transporter** et **protéger** les requêtes DNS en les **chiffrant**
- Ce protocole **empêche la surveillance** ou **la corruption** des messages DNS par des **pirates informatiques**
- Les informations relatives à la navigation **ne sont plus lisibles** ; cela améliore la **confidentialité** et **protège les données** de l'internaute

altrnativ.net

DNS OVER HTTPS .doh

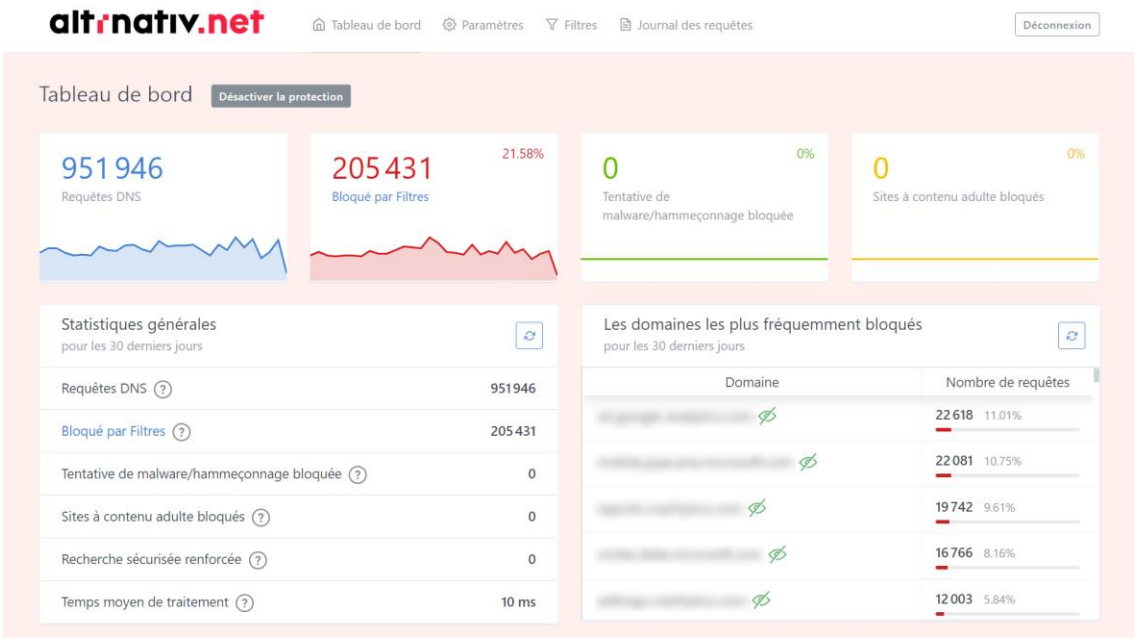
Le service DoH

Pour éviter le problème rencontré par les précédents systèmes où les dispositifs sur le trajet interfèrent avec les DNS *(par exemple le problème classique de blocage des ports).*
DoH est essentiellement HTTPS, le standard chiffré utilisé par le Web, et utilise le même numéro de port (tcp/443). Les navigateurs Web ont déjà désapprouvé le HTTP non sécurisé en faveur du HTTPS. Cela fait du HTTPS un excellent choix pour transporter les messages DNS en toute sécurité.

Il est ainsi possible de résoudre tous les problèmes inerrants à la résolution de nom en utilisant DNS over HTTPS (DoH).

Le protocole de transport DoH va nous permettre de passer à un Internet plus sûr. L'ensemble des adresses IP sont anonymisées et comme les sites visités ne sont pas conservés, sauf si vous le souhaitez pour suivre vos statistiques. (1 / 7 / 30 jours)

Technologie Open Source



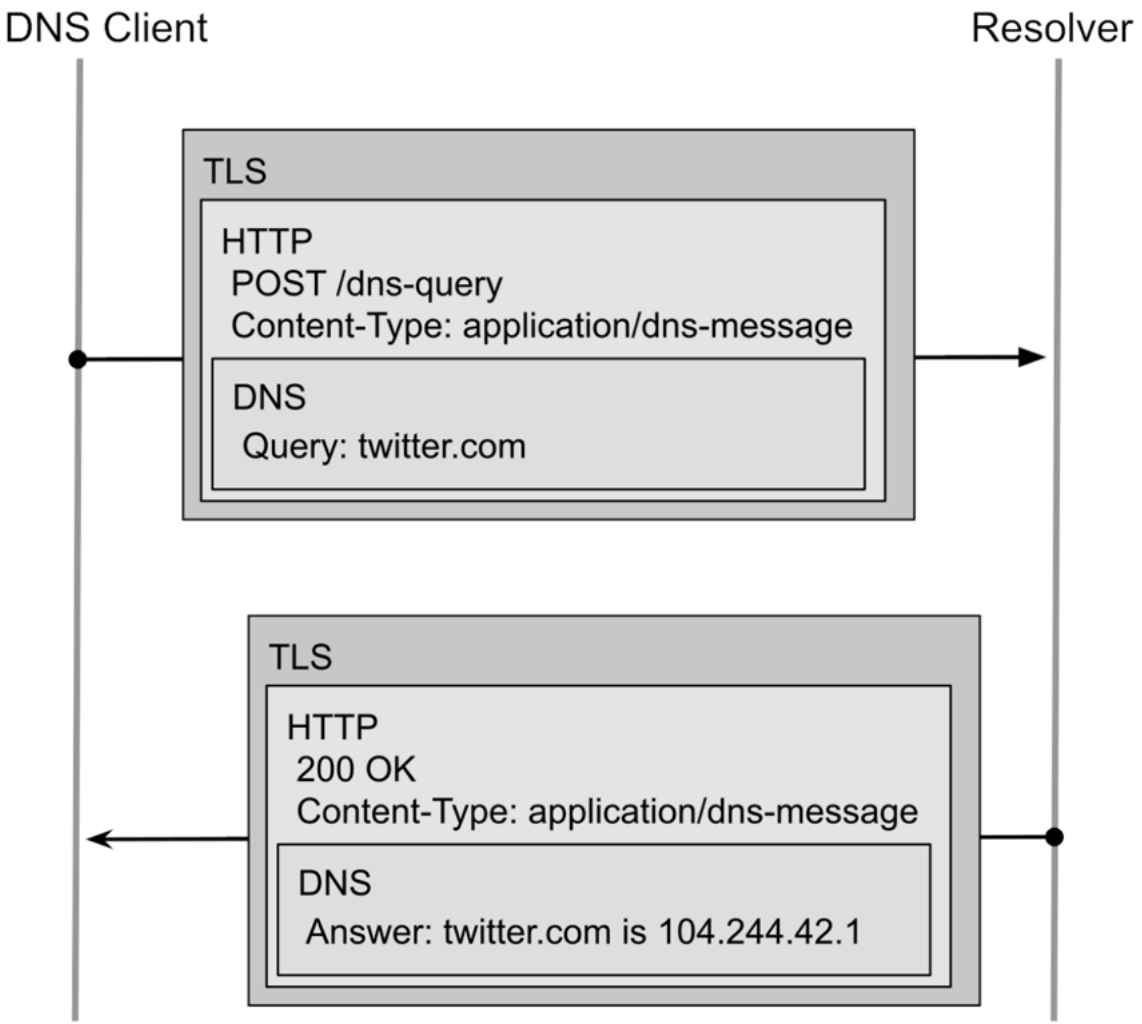
alternativ.net

DNS OVER HTTPS .doh

Chiffrement des DNS

Le fait de chiffrer les requêtes DNS rend beaucoup plus difficile la surveillance de vos messages DNS. Tout comme le Web est passé du HTTP non chiffré au HTTP**S** chiffré, il est désormais possible de mettre à niveau le protocole DNS vers une version chiffrée. Le chiffrement du Web a permis de sécuriser et privatiser les communications et de développer le commerce. Le chiffrement des DNS sera une amélioration supplémentaire de la confidentialité pour les utilisateurs.

Le mécanisme normalisé permettant de sécuriser le transport DNS entre vous et le serveur : DNS Queries over HTTPS est basé sur le protocole Transport Layer Security (TLS) qui est également utilisé pour chiffrer la communication entre vous et le site Web en utilisant HTTPS. Dans le protocole TLS, le serveur (qu'il s'agisse d'un serveur Web ou d'un serveur DNS) s'authentifie auprès du client à l'aide d'un certificat. Ceci garantit que personne d'autre ne puisse se faire passer pour le serveur DNS.



DoH : Requête et réponse DNS transportées via un flux HTTPS sécurisé

altrnativ

Reboot The Net

altrnativ.com