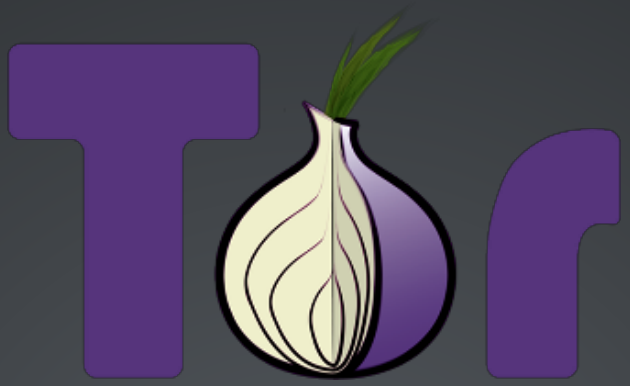


PROTÉGEZ VOTRE ANONYMAT

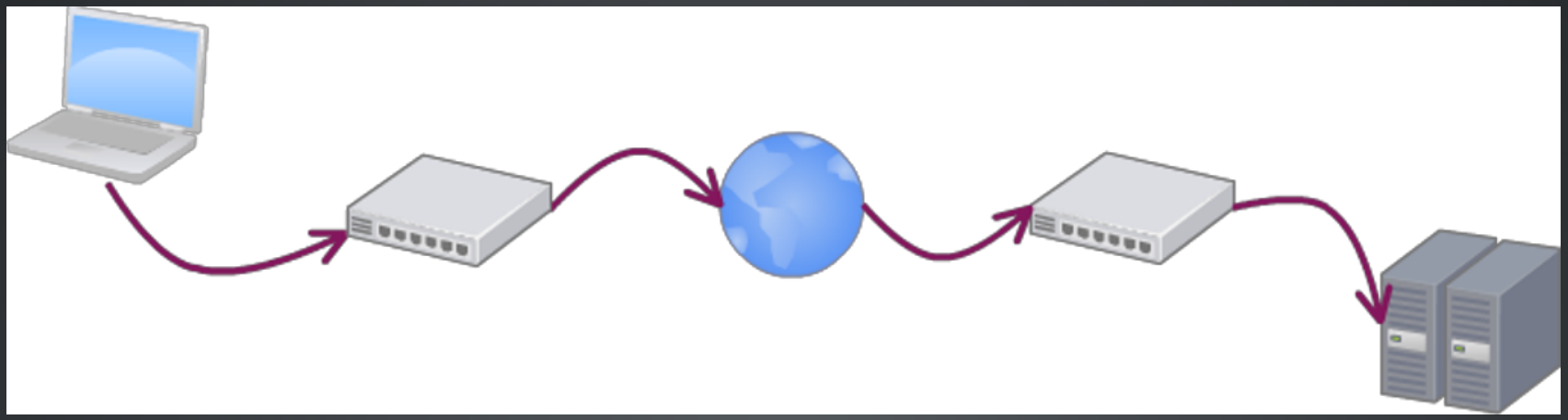
@aeris

17 novembre 2013, Ubuntu Party

SOMMAIRE

1. Fonctionnement
2. Outils
3. Cas d'utilisation
4. Comment aider
5. Questions

COMMUNICATIONS INTERNET



Pleins d'intermédiaires

- FAI
- Fournisseurs de contenu
- Intermédiaires techniques
- Points de peerings
- Câbles sous-marins

Chaque point et chaque lien peut potentiellement être compromis

HTTP

```
Source : 109.190.87.53 (aeris.imirhil.fr)
Destination : 46.51.197.89 (ec2-46-51-197-89.eu-west-1.compute.amazonaws.com)
Requête :
        GET / HTTP/1.1
        Host: duckduckgo.com
Réponse :
        HTTP/1.1 200 OK
        Content-Type: text/html; charset=UTF-8
        <!DOCTYPE html>
        <html>…</html>
```

Le paquet contient tout ce qu'il faut pour espionner

- IP source : 109.190.87.53
- IP destination : 46.51.197.89
- Site consulté : Duckduckgo
- Contenu de la requête
- Contenu de la réponse

HTTPS

```
Source : 109.190.87.53 (aeris.imirhil.fr)
Destination : 46.51.197.89 (ec2-46-51-197-89.eu-west-1.compute.amazonaws.com)
Requête :
        =~IE<!@@M"1$M:
        95I7$80j3O1wZ0>GW<^f.:v"'Hrb74RrY\ZW? V~Iq'm'EXrhzp^[Rd/,
Réponse :
        X5uE'@4."089:'
        i95I#A&(LygK>D)GjMNt8-W7jeM?~VQ<V\(<;EPE@[IUmO;&$K-l%2
```

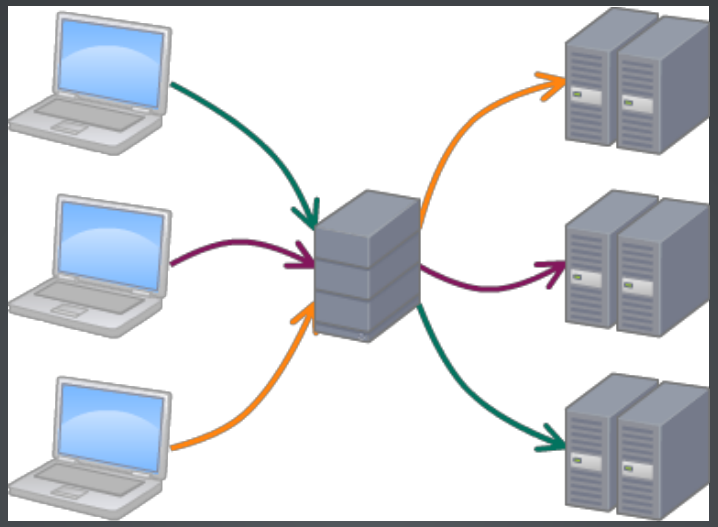
Le paquet contient déjà un peu moins de données sensibles

- IP source : 109.190.87.53
- IP destination : 46.51.197.89
- Site consulté : Duckduckgo  S.N.I.

- Contenu de la requête
- Contenu de la réponse

Peut-on aller plus loin ?

PROXY / VPN



Fondamentalement pas meilleur

- Compromission du prestataire
- Analyse temporelle

TOR À LA RESCOUSSE

LE PROJET TOR

Système de routage en oignon

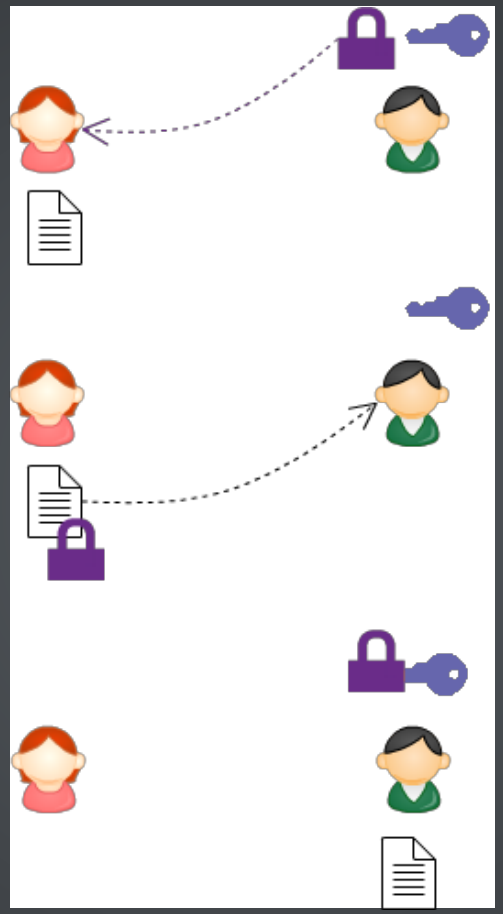
Logiciel libre

1ère version en 2002

Soutenu par *The Tor Project*

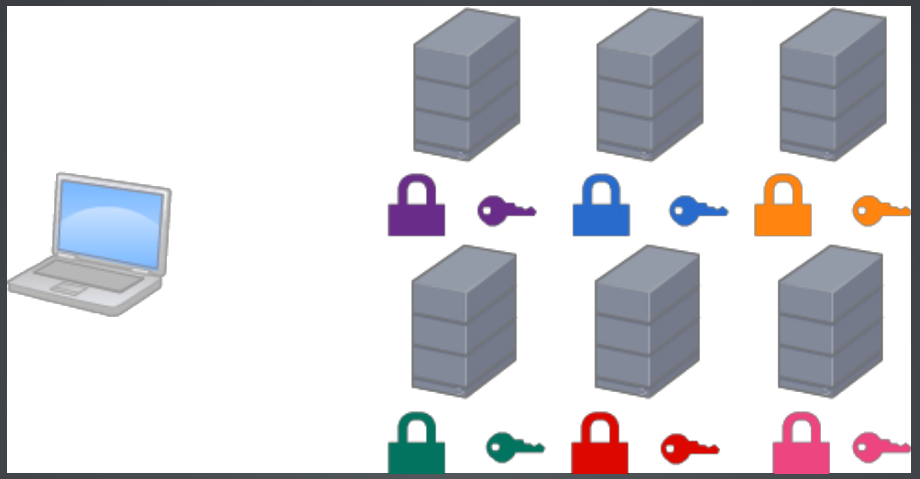
Organisation à but non lucratif

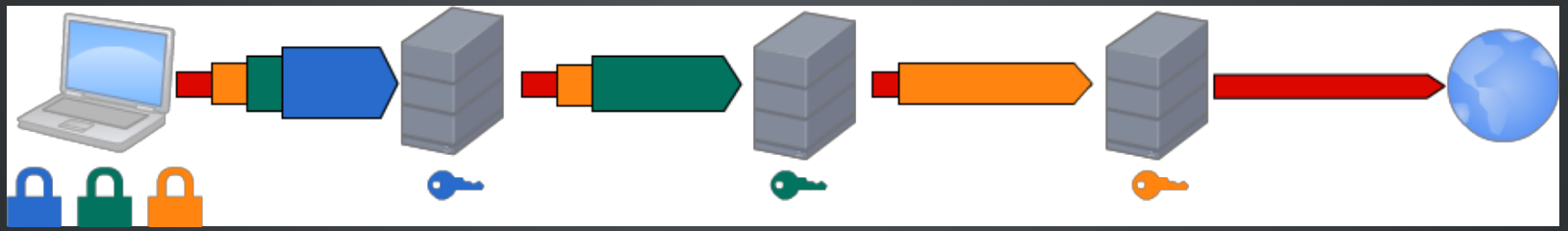
CRYPTOGRAPHIE À CLEF PUBLIQUE



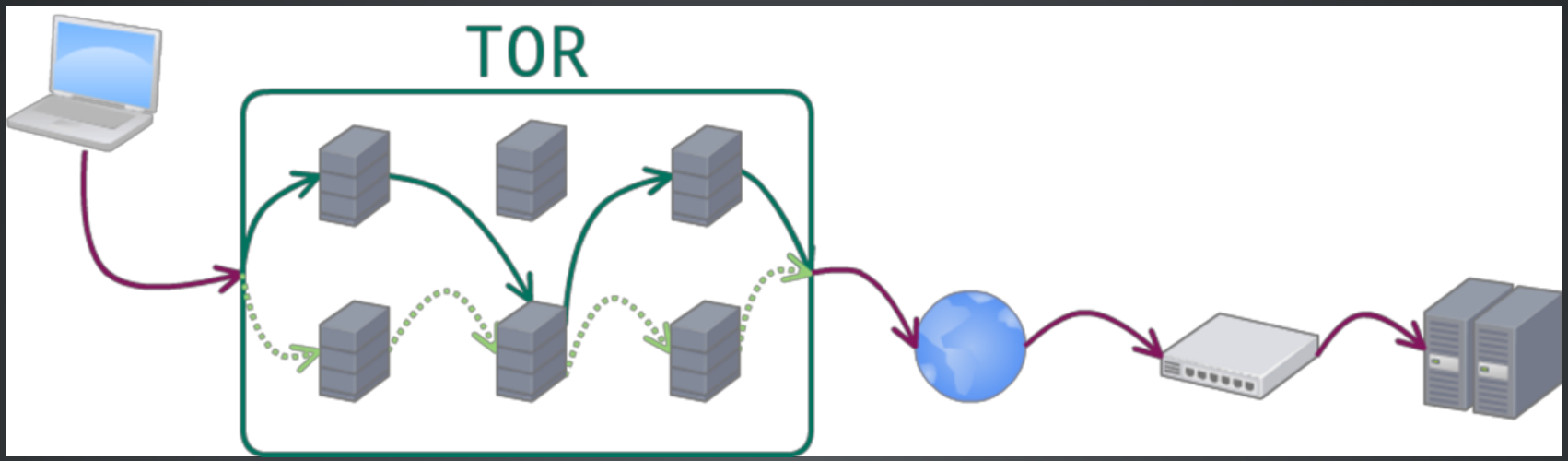
ROUTAGE EN OIGNON

Triple chiffrement à clef publique





COMMUNICATIONS AVEC TOR



	S → G	G → M	M → E	E → C
Source	S.S.S.S	G.G.G.G	M.M.M.M	E.E.E.E
Destination	G.G.G.G	M.M.M.M	E.E.E.E	D.D.D.D
Contenu	5VdN57o	V05IoDU	MTHpBWg	Contenu

Plus personne ne connaît l'intégralité des données

Attention à la sortie ⇨ SSL…

BLOCAGE DE TOR

La liste des nœuds Tor est publique

⇨ blacklist

Utilisation de nœuds non listés

⇨ bridges Tor

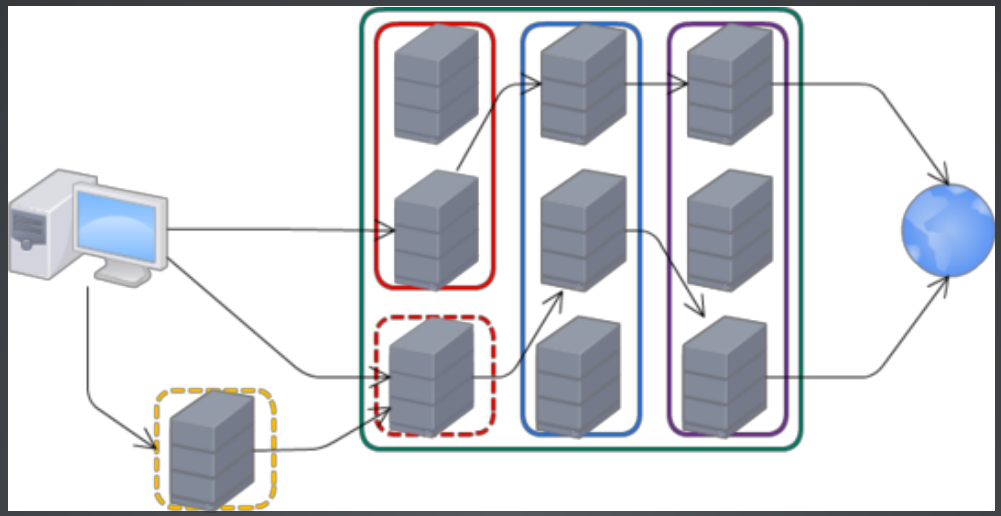
Le trafic Tor est reconnaissable

⇨ Deep Packet Inspection

Encapsulation dans du trafic « neutre »

⇨ obfsproxy 

RÉCAPITULATIF : LES TYPES DE NŒUDS



Guards Nœuds d'entrée publics

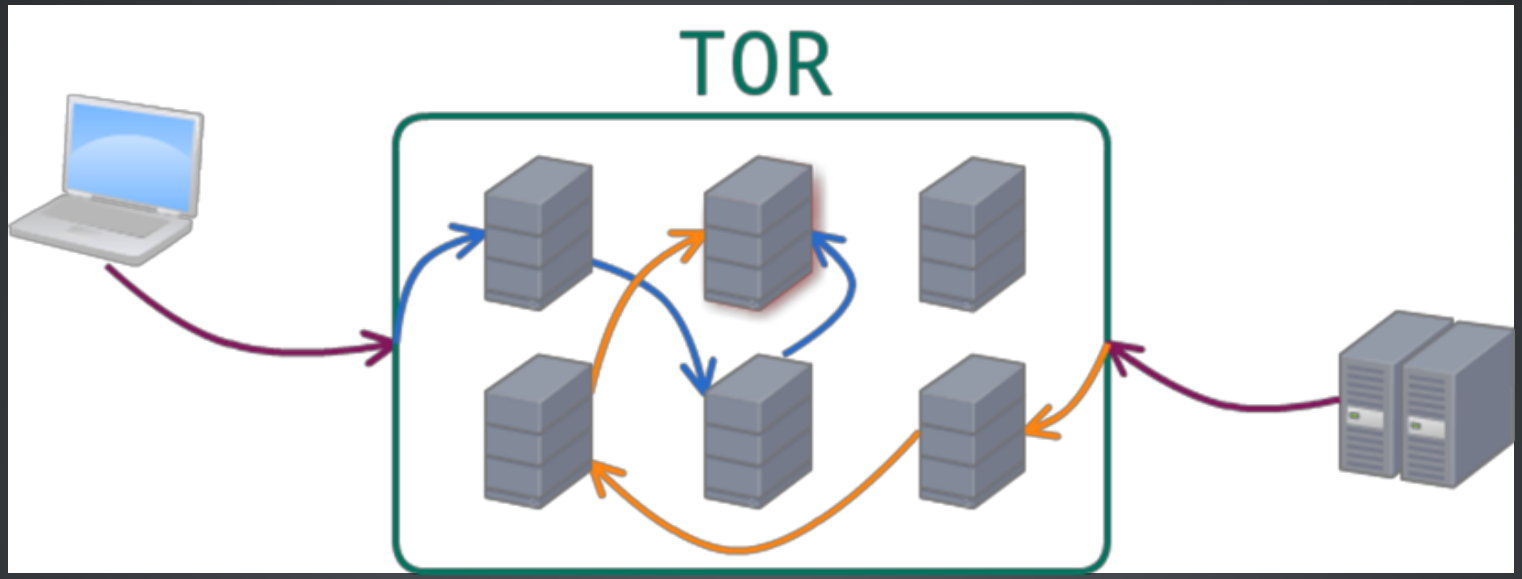
Bridges Nœuds d'entrée privés

Middle Nœuds intermédiaires

Exit Nœuds de sortie

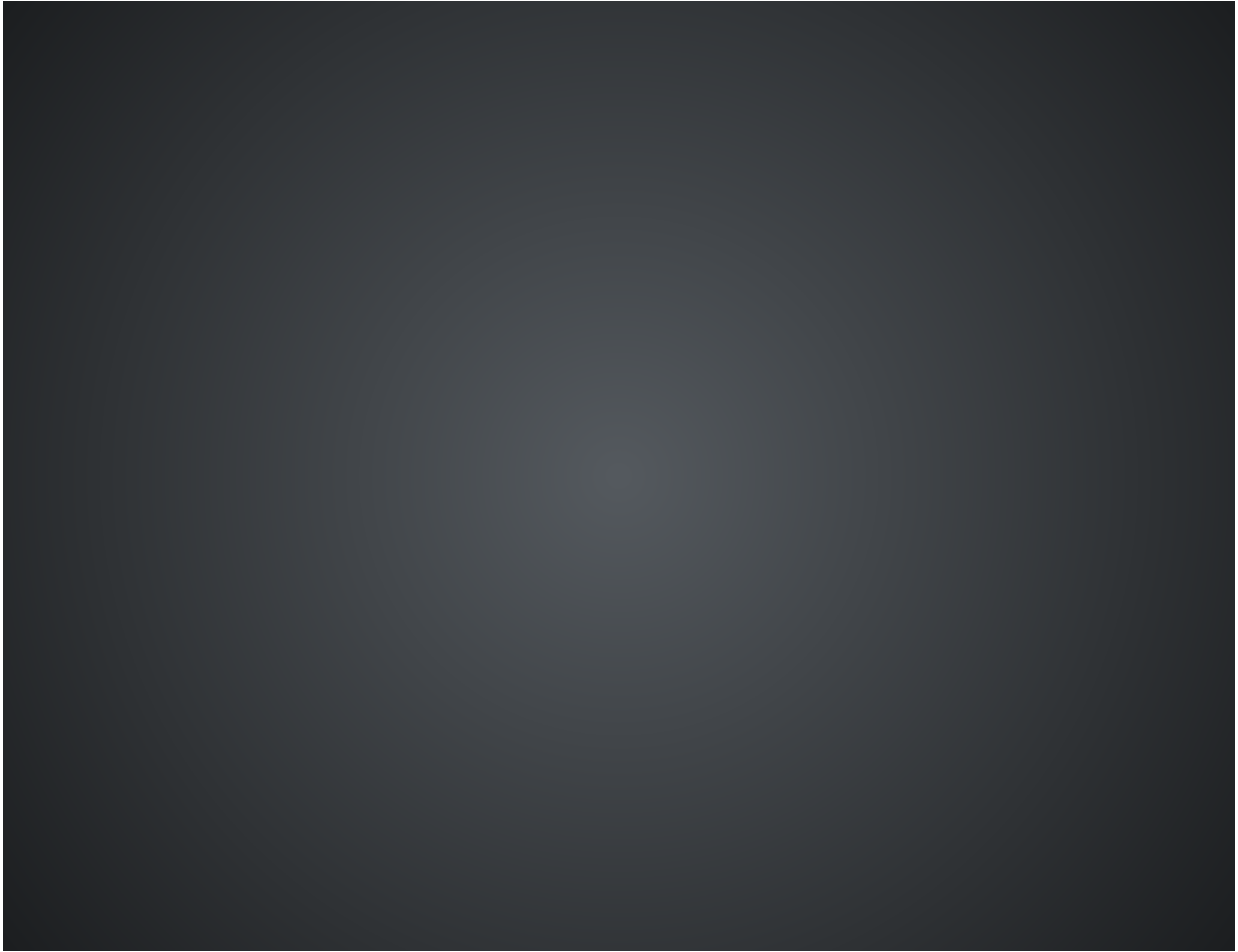
Obfsproxy Nœuds d'obfuscation

SERVICES CACHÉS



- Adresses en *.onion*
- Double routage en oignon
  - 3 relais depuis le client
  - 3 relais depuis le serveur
- Le client ne sait rien du serveur

QUELQUES CHIFFRES



4600 relais présents dans le réseau

900 nœuds de sortie

40Gb/s de bande passante

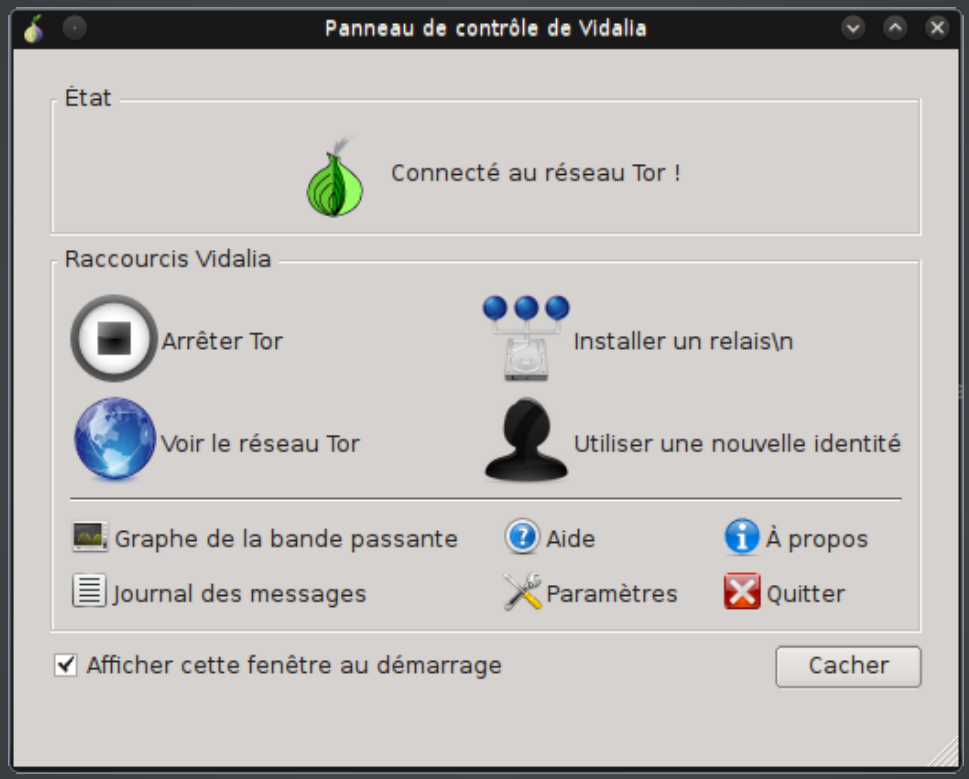
25Gb/s utilisés

500k utilisateurs (6% de Français)

LES OUTILS

GNU/LINUX

Vidalia + Firefox + Foxy Proxy



Contourne la censure

Pas d'anonymat

ANONYMAT ≠ IP

- IP
- User agent
- Historique
- Cookies
- URL externes
- Javascript
- SSL
- Pleins d'autres choses

ANONYMAT

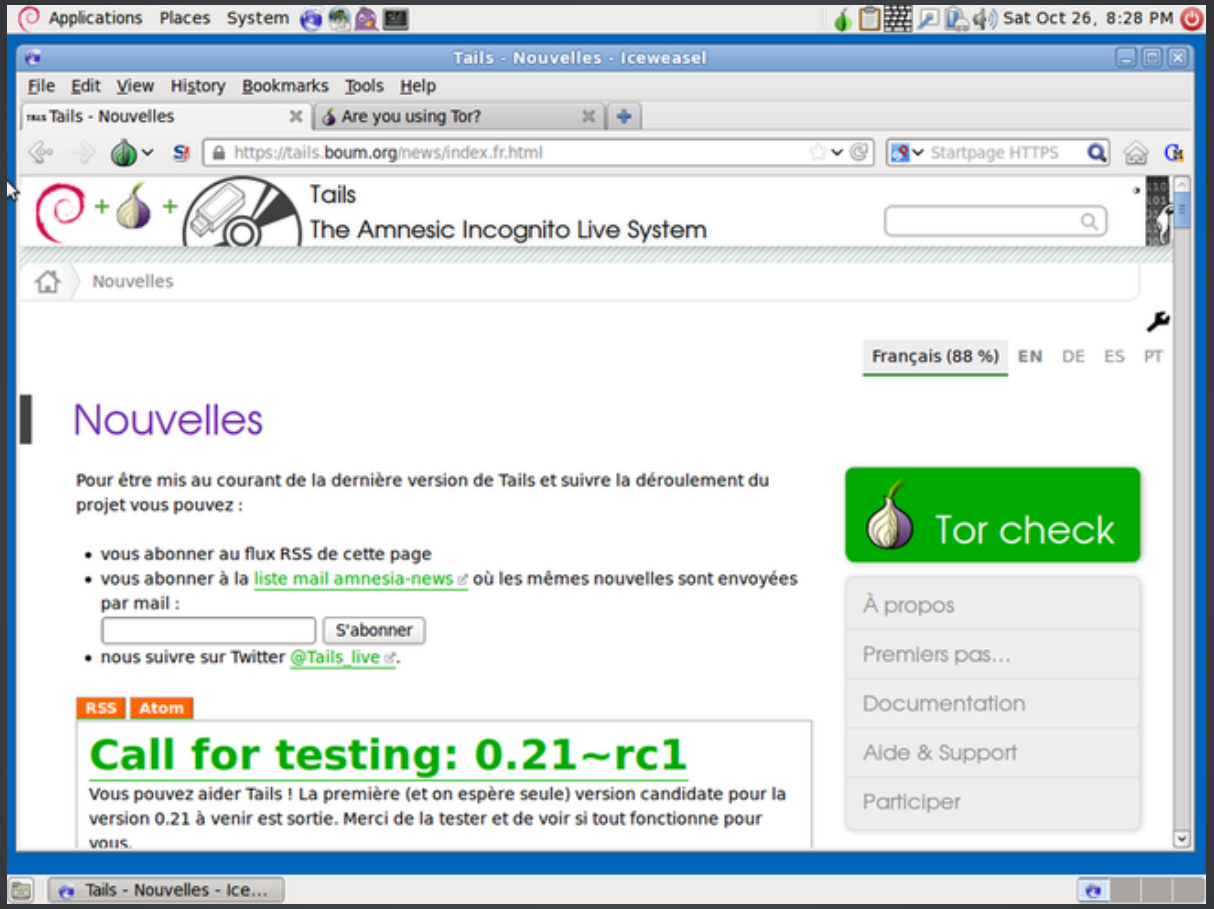
- Modifier son user agent ⇨ User Agent Switcher
- Bloquer les cookies ⇨ Cookie Monster
- Interdire les appels externes
  - ⇨ Request Policy
  - ⇨ Disconnect
  - ⇨ Adblock Edge
- Interdire le javascript ⇨ No Script
- Faire attention aux certificates SSL
  - ⇨ HTTPS Everywhere
  - ⇨ Certificate Patrol
- Des logiciels à jour
- Du bon sens, de la méfiance

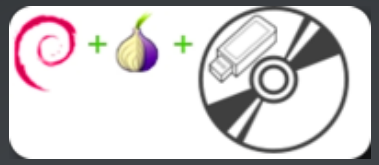
GNU/LINUX

Tor Browser Bundle

Firefox remasterisé

TAILS


Applications Places System
Sat Oct 26, 8:28 PM
Tails - Nouvelles - Iceweasel
File Edit View History Bookmarks Tools Help
Tails - Nouvelles
Are you using Tor?
https://tails.boum.org/news/index.fr.html
Startpage HTTPS
Tails
The Amnesic Incognito Live System
Nouvelles
Français (88 %) EN DE ES PT
Nouvelles
Pour être mis au courant de la dernière version de Tails et suivre la déroulement du projet vous pouvez :
vous abonner au flux RSS de cette page
vous abonner à la liste mail amnesia-news où les mêmes nouvelles sont envoyées par mail :
S'abonner
nous suivre sur Twitter @Tails_live.
RSS Atom
Call for testing: 0.21~rc1
Vous pouvez aider Tails ! La première (et on espère seule) version candidate pour la version 0.21 à venir est sortie. Merci de la tester et de voir si tout fonctionne pour vous.
Tor check
À propos
Premiers pas...
Documentation
Aide & Support
Participer
Tails - Nouvelles - Ice...



TAILS

Live CD/USB Debian axé anonymat & sécurité

Tor mais pas que

- GPG
- Métadonnées
- Pare-feu
- Mode « panic »
- …

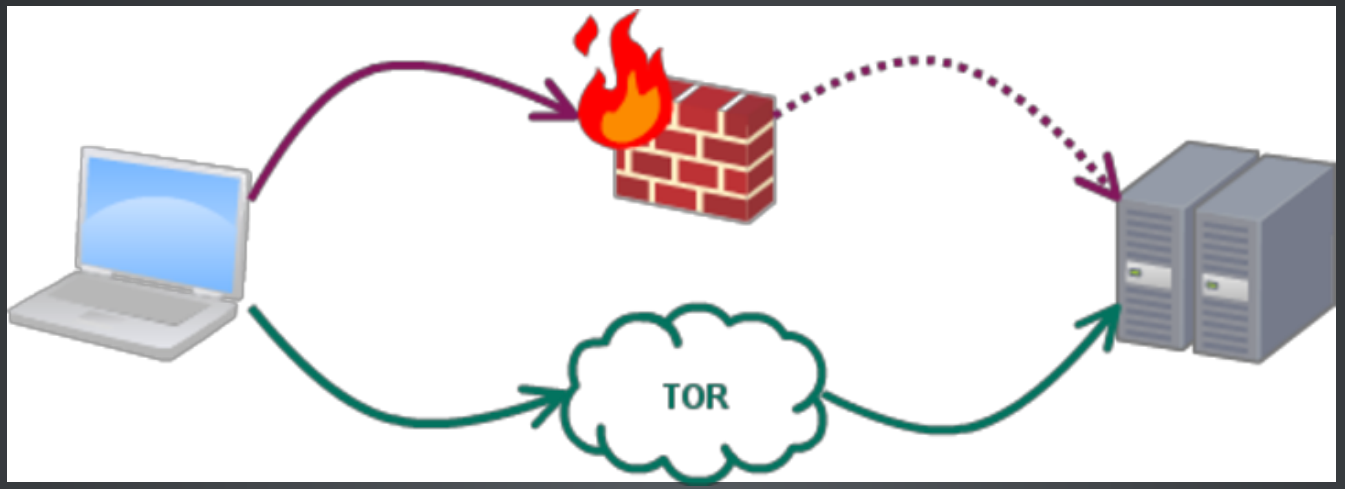
ANDROÏD 

Orbot

WINDOWS / MAC OS 

TOR, POUR QUOI FAIRE ?

CONTOURNER LA CENSURE



Chine, Corée du Nord, Syrie, Russie…

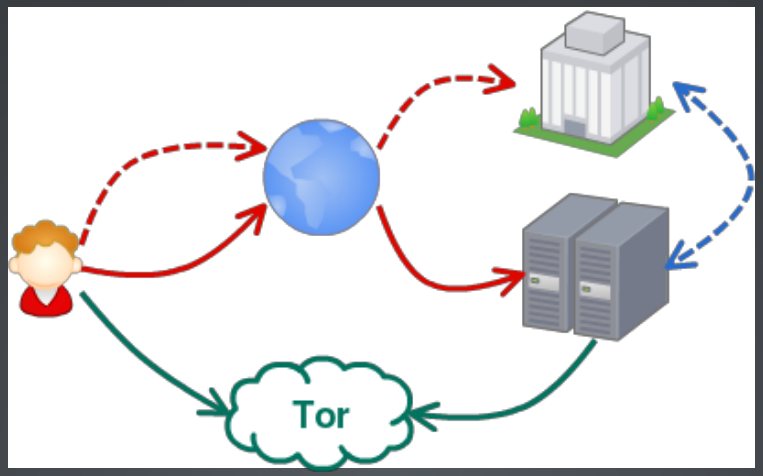
Mais aussi Belgique, France… !!!

On cherche à accéder à du contenu censuré

Contenus illégaux dans le pays en question

⇨ Anonymat souvent nécessaire

ÉVITER LE « DOXING »

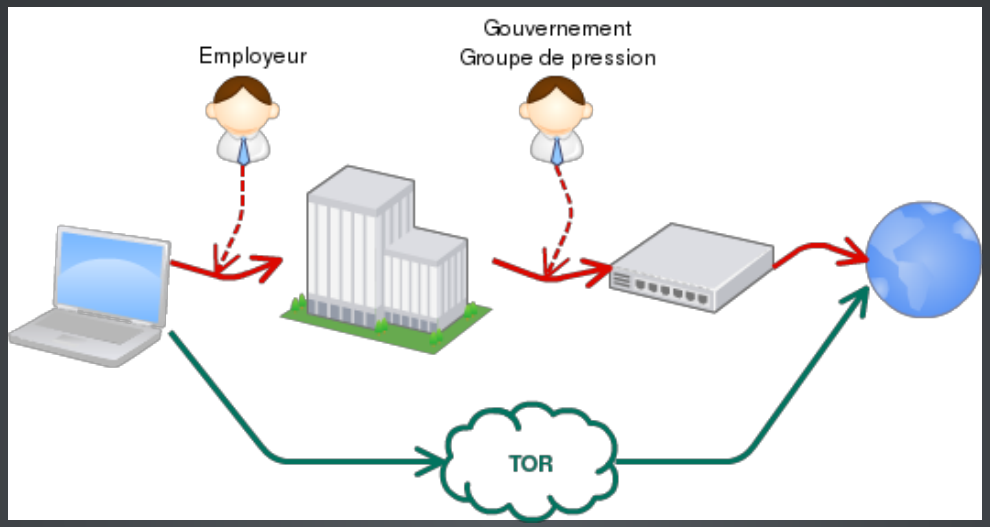


Récupération d'informations personnelles dans un but malveillant

Blog sur des sujets sensibles, positions politiques…

Utilisation de services cachés

PROTECTION DES LANCEURS D'ALERTE



Manning, Snowden et tant d'autres

On doit communiquer des informations sensibles

Risques encourus : perso, pro, juridiques, moraux

On doit continuer à émettre

⇨ Anonymat +++

COMMENT AIDER

HÉBERGER DES NŒUDS DE SORTIE

De la bande passante disponible (≥100Mbs)

S'occuper des mails abuse@

Des risques possibles (convocation, saisie…)

Éviter les actions isolées

Agir collectivement

⇨ 

23 adhérents

Des entrées RIPE

Des bénévoles pour répondre à abuse@

Marcuse : nœud intermédiaire (Liazo, 25/06/2013, 100Mbps)

Ekumen : nœud de sortie (Gandi, 23/10/2013, 100Mbps \o/)

Marcuse : nœud de sortie (Liazo, 15/11/2013, 100Mbps \o/ \o/)

HÉBERGER D'AUTRES TYPES DE NŒUDS

Être nœud de sortie est le plus utile pour le réseau

Mais effets de bord +++

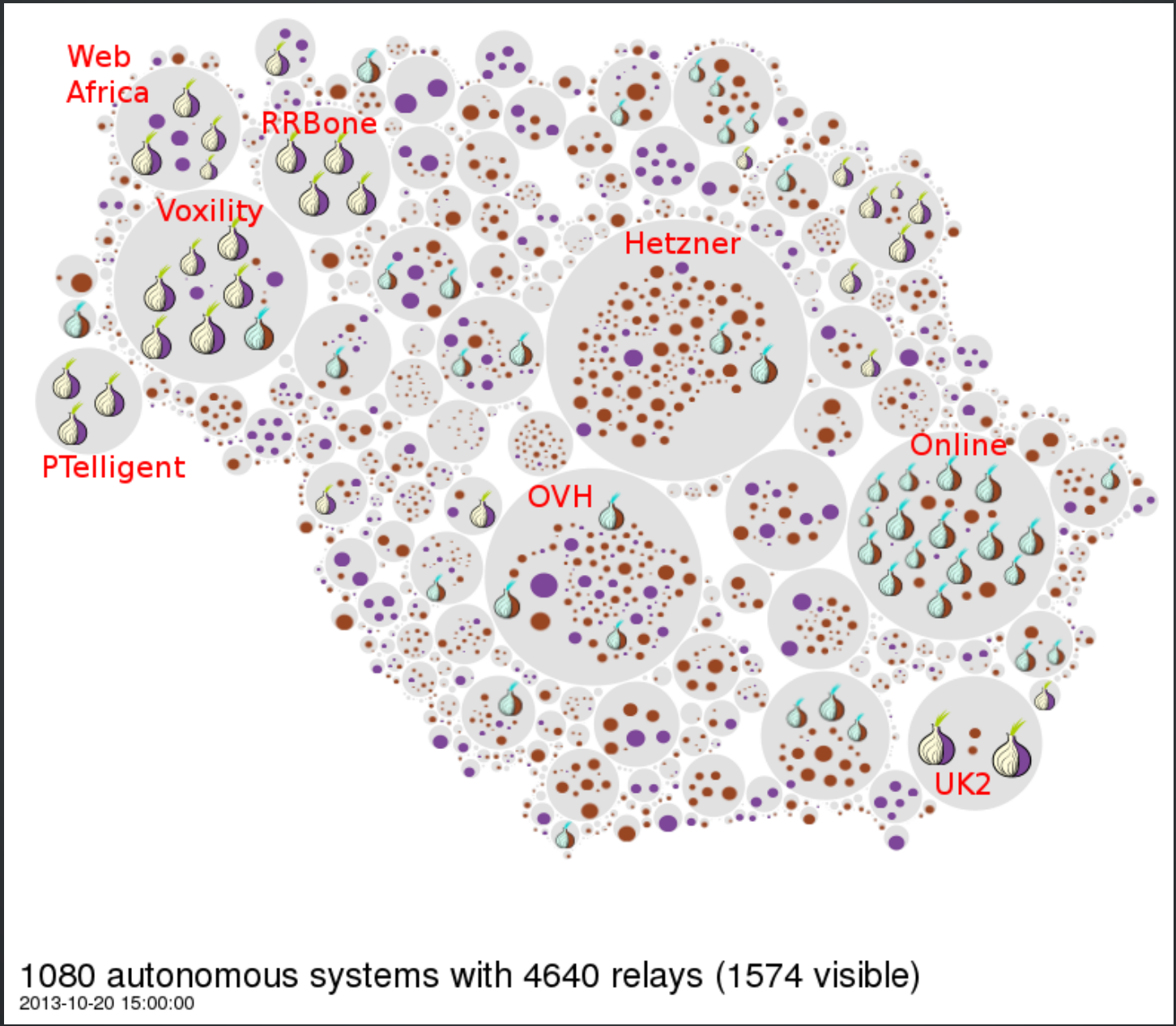
Être middle ou guard

Mais toujours quelques effets de bord

On peut aussi monter des bridges ou des obfsproxy

Pas ou peu d'effets de bord

DIVERSITÉ


Web
Africa
RRBone
Voxility
Hetzner
PTelligent
OVH
Online
UK2
1080 autonomous systems with 4640 relays (1574 visible)
2013-10-20 15:00:00

REJET / INCOMPRÉHENSION

7.4 Pour des raisons de sécurité, OVH se réserve la possibilité de procéder à la suspension immédiate et sans préavis de tout Serveur sur lequel serait proposé à titre gracieux ou onéreux, un service ouvert au public de Proxy, IRC, VPN, TOR, pour lequel OVH aurait connaissance d'une utilisation malveillante, frauduleuse ou illicite.

De plus, dans le cas où le Service mis à disposition de l'Usager :

- Permet relayer des requêtes Internet par un serveur mandataire «Proxy» installé sur le Serveur de l'Usager sans authentification ni identification de l'internaute, en particulier les réseaux «TOR», «FreeNet», «Hacktisvismo» et «A4Proxy»,

ONLINE se réserve, pour protéger l'intégrité de son système d'information, la possibilité d'interrompre immédiatement sans préavis les Services mis à disposition de l'Usager. En outre, l'Usager ne pourra prétendre obtenir d'indemnisation pour les éventuelles pertes de données et/ou interruptions de service qui en résulterait.

⇨ Communication, information

⇨ Neutralité du réseau

QUESTIONS