

What is Internet censorship?

Internet censorship is the **intentional control** or suppression of what can be accessed, published, or viewed on the internet.

OONI measures censorship on the **network** level, involving the **blocking of websites and apps**.

Why measure Internet censorship?

- 1 Check/confirm reports
- 2 Uncover information controls
- 3 Transparency and oversight
- 4 Collect evidence of information controls



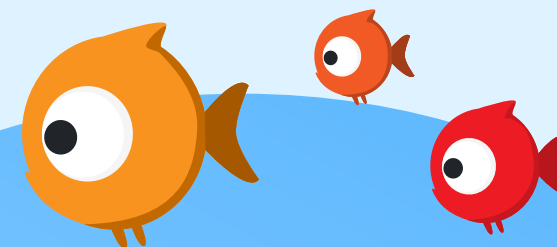
Comprendre la censure de l'Internet

Explorer les Restrictions Web et Contrôle d'Accès



Founded in 2012, the Open Observatory of Network Interference (OONI) is a non-profit free software project documenting Internet censorship around the world.

Learn more about OONI: ooni.org



Qui met en oeuvre la censure de l'Internet?

Les Fournisseurs d'Accès Internet (FAI) utilisent une variété de techniques de censure. Parmi elles, le **trucage DNS**, le **blocage IP**, le **filtrage SNI**.

Comment la censure d'Internet est-elle mise en oeuvre?

Les **fournisseurs d'Accès Internet (FAI) bloquent l'accès à des sites web ou applications spécifiques** se basant sur des ordonnances gouvernementales conformément à la législation nationale.

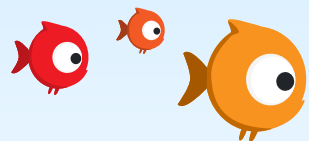
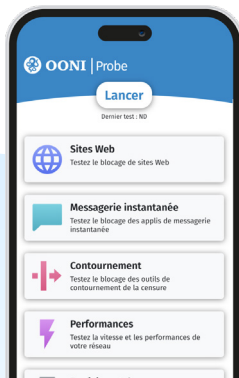
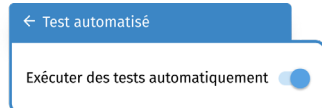
Comment mesurer la censure de l'Internet?

Obtenir l'app **OONI Probe** sur Mobile et Ordinateur.

| Scanner pour installer OONI Probe →



Activer **Test Automatisé** dans les paramètres pour exécuter des tests automatiquement chaque jour!



Trucage DNS

Le trucage DNS se produit lorsque les Fournisseurs d'Accès Internet (FAI) interfèrent avec la résolution DNS pour un nom d'hôte particulier, vous empêchant d'y accéder (Ex:en renvoyant la mauvaise adresse IP).

Blocage HTTP

Le blocage HTTP se produit lorsqu'un FAI **interfère avec la connexion entre votre ordinateur et le serveur hébergeant le site web** auquel vous essayez d'accéder.

Ceci est mis en oeuvre en interceptant votre requête HTTP (dans certains cas, vous redirigeant vers une page de blocage) ou en fermant la connexion (empêchant ainsi l'échange normal entre votre ordinateur et le serveur du site web).

Blocage IP

Le blocage IP survient lorsque les Fournisseurs d'Accès Internet (FAI) **bloquent les connexions à l'adresse IP** d'un site web.



Filtrage basé sur le SNI

SNI est une extension du protocole TLS (utilisé pour les sites web hébergés sur HTTPS), conçu pour spécifier le nom d'hôte avec lequel la connexion cryptée doit être établie.

Comme le champ SNI est non crypté, les Fournisseurs d'Accès Internet sont en mesure de voir si vous essayez d'accéder à un site web banni et de restreindre l'accès.

La censure indentifiée par le **champ SNI** est caractérisée comme filtrage basé sur le SNI

Méthode de détection	Méthode de blocage					
	Fermer la connexion (RST ou FIN)	Abandon de Paquet	Etrangelement de trafic	MITM	Mauvaise réponse HTTP	Mauvaise réponse DNS
Destination IP (+ port)	✓	✓	✓	✓		
Domaine dans la requête DNS						✓
Entête d'hôte HTTP	✓	✓	✓	✓	✓	
SNI déposé dans la poignée de main TLS	✓	✓	✓	✓		