Perspectives de l'Internet Society sur le blocage de contenu sur Internet : tour d'horizon

Mars 2017

Internet Society

Table des matières

Avant-propos

L'utilisation du blocage d'Internet par les gouvernements pour empêcher l'accès aux contenus illégaux est une tendance mondiale et en hausse. Il existe de nombreuses raisons pour lesquelles les décideurs politiques choisissent de bloquer l'accès à certains contenus tels que le jeu de hasard en ligne, la propriété intellectuelle, la protection de l'enfance et la sécurité nationale. Cependant, en dehors des questions liées à la pornographie juvénile, il existe peu de consensus international sur ce qui constitue un contenu approprié du point de vue des politiques publiques.

L'objectif de cet article est de fournir une évaluation technique des différentes méthodes de blocage de contenu sur Internet, y compris la façon dont chaque méthode fonctionne et quels sont les limites et les problèmes associés à chacune d'elles. Nous ne cherchons pas à évaluer la légalité ou les motivations politiques du blocage de contenu sur Internet[1].

Notre conclusion, basée sur des analyses techniques, est que l'utilisation du blocage d'Internet pour lutter contre des contenus ou des activités illicites est dans l'ensemble inefficace, souvent sans effets et entraîne généralement des dommages collatéraux aux internautes.

D'un point de vue technique, nous recommandons aux décideurs politiques de réfléchir à deux fois lorsqu'ils envisagent l'utilisation d'outils de blocage de contenus sur Internet dans l'objectif de résoudre des problèmes de politiques publiques. S'ils choisissent de poursuivre des approches alternatives, cela constituera une victoire importante pour un Internet global, ouvert, interopérable et fiable.

1 Les lecteurs intéressés par les évaluations juridiques du blocage de contenu peuvent consulter les ressources suivantes :
- Article 19 : https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf
- Conseil de l'Europe : http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

Introduction

L'évolution de l'Internet en tant que phénomène sociétal mondial doit beaucoup aux contenus et aux services qui ont tiré parti de l'architecture unique du réseau. Des pays entiers dépendent des flux de contenu transfrontaliers. Des innovations quotidiennes ont le potentiel de remettre en cause l'existence d'industries entières. L'Internet est désormais un facteur clé des processus démocratiques et des discussions politiques. Des relations personnelles sont créées et rompues en ligne.

La tendance ne ralentit pas. Selon les estimations[2], le trafic Internet global en 2020 équivaudra à 95 fois le volume de l'Internet global en 2005. Le nombre d'appareils connectés aux réseaux IP sera trois fois plus élevé que la population mondiale en 2020.

Pourtant, Internet contient également du contenu que les décideurs politiques, les législateurs et les régulateurs du monde entier veulent bloquer. Du blocage des sites de jeux de hasard étrangers en Europe et en Amérique du Nord au blocage de discours politique en Chine, l'utilisation de techniques de blocage de contenu sur Internet pour empêcher l'accès à du contenu considéré comme illégal en vertu de certaines lois nationales est un phénomène mondial. Les motivations basées sur des considérations de politiques publiques dans le but de bloquer le contenu de l'Internet sont diverses, allant de la lutte contre la violation de la propriété intellectuelle, le matériel d'abus d'enfants et les activités illégales en ligne, à la protection de la sécurité nationale.

L'objectif de cet article n'est ni d'évaluer ces motivations ni de qualifier si un certain type de blocage est bon ou mauvais d'un point de vue éthique, juridique, économique, politique ou social. Nous proposons plutôt une évaluation technique des avantages et des inconvénients des techniques de blocage les plus couramment utilisées pour empêcher l'accès au contenu jugé illégal. L'objectif est d'aider les lecteurs à comprendre ce que chaque technique peut et ne peut pas bloquer, ainsi que les effets secondaires, les limites, les compromis et les coûts associés.

Notre conclusion est que l'utilisation des méthodes de blocage sur Internet pour lutter contre les contenus illégaux est dans l'ensemble inefficace, souvent sans effets et susceptible de causer des dommages collatéraux non intentionnels aux internautes (voir le résumé plus loin dans le tableau de la page 6).

D'un point de vue technique, **nous appelons les décideurs politiques à réfléchir à deux fois** avant de préconiser ces mesures et les invitons à axer leurs réponses en se concentrant en priorité sur des mesures alternatives ciblées sur le problème à sa source (voir les recommandations plus détaillées à la fin de cet article, y compris des conseils sur la façon de minimiser les effets négatifs de ces mesures).

Il convient également de noter que ce document ne se concentre pas sur les mesures de blocage mises en œuvre pour des raisons de sécurité ou de gestion régulière de réseau (p. ex. combat contre les pourriels/spam, logiciels malveillants). Dans de tels cas, certains des mêmes outils que nous décrivons dans cet article peuvent souvent être efficaces pour atteindre les objectifs visés.

Encadré :
Filtrage, blocage ou censure ?

Pour décrire le filtrage d'Internet, des termes tels que « filtrage », « blocage», « coupure » et « censure » sont fréquemment utilisés (parmi d'autres). Du point de vue de l'utilisateur, le terme choisi est moins important que l'effet : une partie d'Internet est inaccessible. Pour les décideurs politiques et les activistes numériques, le choix d'un terme particulier est plutôt motivé par la sémantique que par l'exactitude technique. Le mot « censure » porte une forte connotation négative, tandis que le « filtrage » semble être une opération plus douce et inoffensive, comme l'élimination des pépins indésirables d'un verre de jus d'orange. Nous avons choisi d'utiliser le mot « blocage » comme un terme simple et direct tout au long de cet article.

2 Index de réseau virtuel Cisco® : http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

Le tableau ci-dessous résume les principaux inconvénients associés au blocage de contenu mandaté sur la base de considérations de politiques publiques :

Problème	Détails
Contournement aisé	Toutes les techniques décrites dans cet article peuvent être déjouées par des utilisateurs suffisamment motivés. À mesure que les utilisateurs découvrent les nombreuses façons de contourner le blocage du contenu, l'efficacité du blocage sera réduite.
Ne résout pas le problème	Le blocage du contenu ne supprime pas le contenu considéré comme illégal. Dans certains cas, une interdiction au niveau national peut être incompatible avec les normes internationales. Mais lorsqu'il existe un large consensus sur les contenus illégaux, la meilleure solution au problème est l'élimination du contenu à sa source.
Provoque des dommages collatéraux	Lorsque des contenus légaux et illégaux partagent la même adresse IP, nom de domaine ou d'autres caractéristiques, le blocage du contenu bloquera l'accès à tout : légal ou illégal. Par exemple, bloquer l'accès à un seul article de Wikipedia à l'aide du filtrage DNS bloquera également des millions d'autres articles de Wikipedia.
Expose les internautes à des risques	Lorsque le service Internet local n'est pas considéré comme fiable et ouvert, les internautes peuvent utiliser des approches alternatives et non standard, comme le téléchargement de logiciels qui redirigent leur trafic afin d'éviter les filtres. Ces solutions de fortune exposent les internautes à des risques sécuritaires supplémentaires.
Encourage le manque de transparence	Un environnement transparent et fiable est important pour le bon fonctionnement d'Internet. Le blocage du contenu élimine cette transparence, compromettant la nature ouverte du réseau et provoquant la méfiance des sources d'informations publiques.
Stimule les services alternatifs	Lorsque le blocage de contenu se généralise, des services « souterrains » et des structures alternatives superposées au réseau seront mises en place, abritant le contenu aux yeux de la loi. Par exemple, le contenu peut se déplacer vers le Web invisible (Dark Web) ou les utilisateurs peuvent faire passer le trafic par des VPN.
S'immisce dans la vie privée	Plusieurs types de blocage de contenu nécessitent l'examen du trafic de l'utilisateur, y compris le trafic chiffré. Lorsque des tiers surveillent ce que font les internautes, enregistrent des transactions ou affaiblissent la sécurité de cryptage de base d'Internet, la confidentialité des utilisateurs est violée.
Soulève des préoccupations sur les droits de l'Homme et le traitement équitable	Mis en œuvre sans tenir compte des notions telles que la nécessité et la proportionnalité, le blocage du contenu peut causer des dommages collatéraux importants, limiter les communications libres et ouvertes, et imposer des limites aux droits des individus.

Motivations pour le blocage de contenu

Dans cet article, nous nous concentrons sur les mesures de blocage motivées par des considérations de politiques publiques et de ses effets sur Internet et les internautes (voir l'encadré pour d'autres motivations pour le blocage du contenu).

Le blocage sur la base de considérations de politiques publiques est utilisé par les autorités nationales pour restreindre l'accès à l'information (ou aux services connexes) qui est illégale dans une juridiction particulière, considérée comme une menace pour l'ordre public, ou encore susceptible d'être répréhensible pour un public particulier.

Par exemple, il existe dans la plupart des pays un désir commun de bloquer l'accès des enfants au contenu obscène ou l'accès de tout le monde à des contenus relatifs aux abus d'enfants. Selon l'environnement juridique local, le contenu peut également être bloqué s'il viole les lois sur la propriété intellectuelle, est considéré comme une menace pour la sécurité nationale ou est interdit pour des raisons culturelles ou politiques.

L'un des défis qui amène les autorités nationales à utiliser les mesures de blocage de contenu sur Internet est que les différents acteurs qui participent à l'acheminement du contenu vers les consommateurs peuvent se trouver dans différents pays, avec des lois différentes couvrant ce qui est ou n'est pas un « contenu illégal ». En outre, l'environnement global d'Internet rend la suppression du contenu illégal à sa source plus compliquée que la simple fermeture d'un serveur local. Par exemple, la personne qui fournit le contenu, les serveurs hébergeant le contenu et, enfin, le nom de domaine qui pointe vers le contenu peuvent se trouver dans trois pays différents, au-delà de la compétence d'une autorité nationale. Cela souligne l'importance de la coopération entre les juridictions et la nécessité d'une coordination étroite avec les parties prenantes non gouvernementales.

Autres types de motivation pour bloquer le contenu

Dans cet article, nous nous concentrons sur le blocage sur la base des considérations de politiques publiques, mais il existe deux autres raisons communes pour lesquelles des mesures de blocage sur le réseau sont mises en place. La première est de prévenir et répondre aux menaces de sécurité réseau. Ce type de blocage est très fréquent. Par exemple, la plupart des entreprises tentent d'empêcher les logiciels malveillants d'entrer dans leurs réseaux. De nombreux fournisseurs d'accès à Internet (FAI) bloquent le trafic malveillant quittant leurs réseaux, tels que des objets connectés infectés (p. exwebcams). Le filtrage des courriels est extrêmement fréquent et comprend le blocage des courriels indésirables (spam) ainsi que des courriels malveillants tels que les messages d'hameçonnage (phishing). Ces types de blocage ne sont pas abordés dans ce document.

Une deuxième raison pour le blocage est la gestion de l'utilisation du réseau. Plutôt que viser sur des types particuliers de contenu, la gestion du réseau, de la bande passante ou du temps sont des domaines qui génèrent une utilisation croissante des mesures de blocage de contenu, par exemple, les employeurs peuvent souhaiter restreindre l'accès aux sites de réseaux sociaux pour leurs employés tout en offrant un accès Internet au bureau. Les FAI peuvent bloquer ou autoriser, ralentir ou accélérer certains contenus en fonction de services contractuels. La gestion de l'utilisation du réseau est rarement une question de politique publique, sauf lorsqu'elle entre dans le domaine de comportements anticoncurrentiels. Les lecteurs intéressés par la question de la neutralité du net trouveront des références dans Pour plus d'informations, page 26.

Vue d'ensemble des techniques de blocage de contenu

Chaque technique comporte des limites et implications techniques et politiques qui doivent être prises en compte lorsque des mesures de blocage de contenu sont considérées. L'objectif de cet article est de fournir une méthode commune afin d'évaluer leur efficacité et leurs effets secondaires. Les lecteurs intéressés par une discussion plus technique sur le blocage de contenu trouveront des références aux documents techniques IETF dans Pour plus d'informations, page 26.

Cet article évaluera les types de blocage de contenu suivants :

- Blocage de protocoles et d'adresses IP
- Blocage DPI (Deep Packet Inspection, inspection en profondeur des paquets)
- Blocage d'URL
- Blocage sur plateforme (en particulier les moteurs de recherche)
- Blocage DNS

Nous avons choisi ces cinq types de blocage parce qu'ils représentent les éléments d'un cycle typique de recherche et récupération d'informations par les internautes, y compris l'utilisation d'un moteur de recherche et l'affichage d'informations avec un navigateur Web ou un outil similaire. Ce cycle est très familier aux décideurs politiques, eux-mêmes utilisateurs d'Internet, et ce sont les opérations que la plupart des blocages fondés sur des considérations de politiques publiques tentent de perturber.

Dans le schéma ci-dessous, nous montrons les étapes qu'un internaute typique pourrait suivre pour trouver des informations, ainsi que les types de blocages qui ont été utilisés pour perturber ce cycle. Dans notre schéma, un internaute cherche un certain type de contenu à l'aide d'un moteur de recherche (étape 1), un point de départ commun. Le moteur de recherche renvoie un ensemble de résultats (étape 2), l'utilisateur en sélectionne un et clique sur le résultat (étape 3). Un type de blocage, le blocage sur plateforme, est utilisé pour perturber cette partie du cycle en bloquant certains résultats revenant du moteur de recherche.

L'ordinateur de l'utilisateur essaie de trouver le serveur hébergeant le contenu dans le DNS de l'Internet (étapes 4 et 5). Un deuxième type de blocage, le blocage DNS, est utilisé pour perturber cette partie du cycle.

Ensuite, le navigateur Web de l'utilisateur tente de se connecter au serveur (étape 6). Cette partie du cycle peut être bloquée à l'aide de trois autres types de blocage : le blocage de protocoles et d'adresses IP, le blocage d'URL et le blocage DPI (Deep Packet Inspection, inspection en profondeur des paquets).

Vue d'ensemble : étapes de récupération et blocage des informations en ligne

1. L'utilisateur recherche « bombe » à l'aide du moteur de recherche.
2. Sans filtrage, l'utilisateur voit un résultat
3. L'utilisateur clique sur un résultat (http:/ exemple.com/ bombe)
4. L'ordinateur de l'utilisateur recherche « exemple.com » dans DNS afin de se connecter au serveur Web.
5. exemple.com = 192.0.222
6. Le navigateur Web de l'utilisateur se connecte au serveur Web « exemple.com » et demande la page Web spécifique sur laquelle l'utilisateur a cliqué.
7. De : 192.0.222 — Demande du serveur exemple.com à l'utilisateur — Obtenir :

exemple.com ? DNS RÉSOLVEUR

À : 192.0.222 — Demande du PC de l'utilisateur au serveur exemple.com — Obtenir : http:// exemple.com/bombe

Si le blocage se produit, voici ce que l'utilisateur pourrait voir à la place :

Avec le **filtrage de recherche** et autres blocages sur plateformes, les résultats sont conservés hors de portée de l'utilisateur, s'il utilise un moteur spécifique.	Avec le **blocage DNS,** l'ordinateur de l'utilisateur ne peut pas trouver le serveur et ne peut donc pas se connecter pour voir la page Web. L'utilisateur verra « serveur introuvable ».	Avec le **blocage de protocoles et d'adresses IP,** la connexion au serveur avec IP = 192.0.222 est bloquée. Tout le contenu du serveur est indisponible, que ce soit intentionnellement ou non.	Avec le **blocage d'URL,** le trafic est bloqué si l'URL est trouvée sur la liste de blocage.	Avec le **blocage DPI (Deep Packet Inspection, inspection en profondeur des paquets),** les mots-clés sur la page Web peuvent déclencher une interruption de trafic. Il existe un risque élevé de bloquer du contenu non ciblé.
Aucun résultat trouvé pour « bombe »	**Serveur introuvable**	**La connexion a expiré**	**Ce site a été bloqué par l'administrateur du réseau**	**La connexion a été réinitialisée**

Bien sûr, l'Internet ne se réduit pas aux moteurs de recherche et aux navigateurs Web, et bon nombre des techniques décrites ci-dessous sont efficaces pour bloquer bien plus que des pages Web. Par exemple, l'utilisation de VPN (Virtual Private Netowkrs) pour chiffrer et masquer le trafic peut souvent être bloquée en utilisant une combinaison de blocage DPI et de blocage de protocoles/adresses IP.

Ces types de blocages peuvent être appliqués très précisément (comme un document particulier sur un site Web particulier) ou de manière très générique (comme « contenu couvrant une thématique » ou « services de Voix sur IP »).

Où se produit le blocage de contenu ?

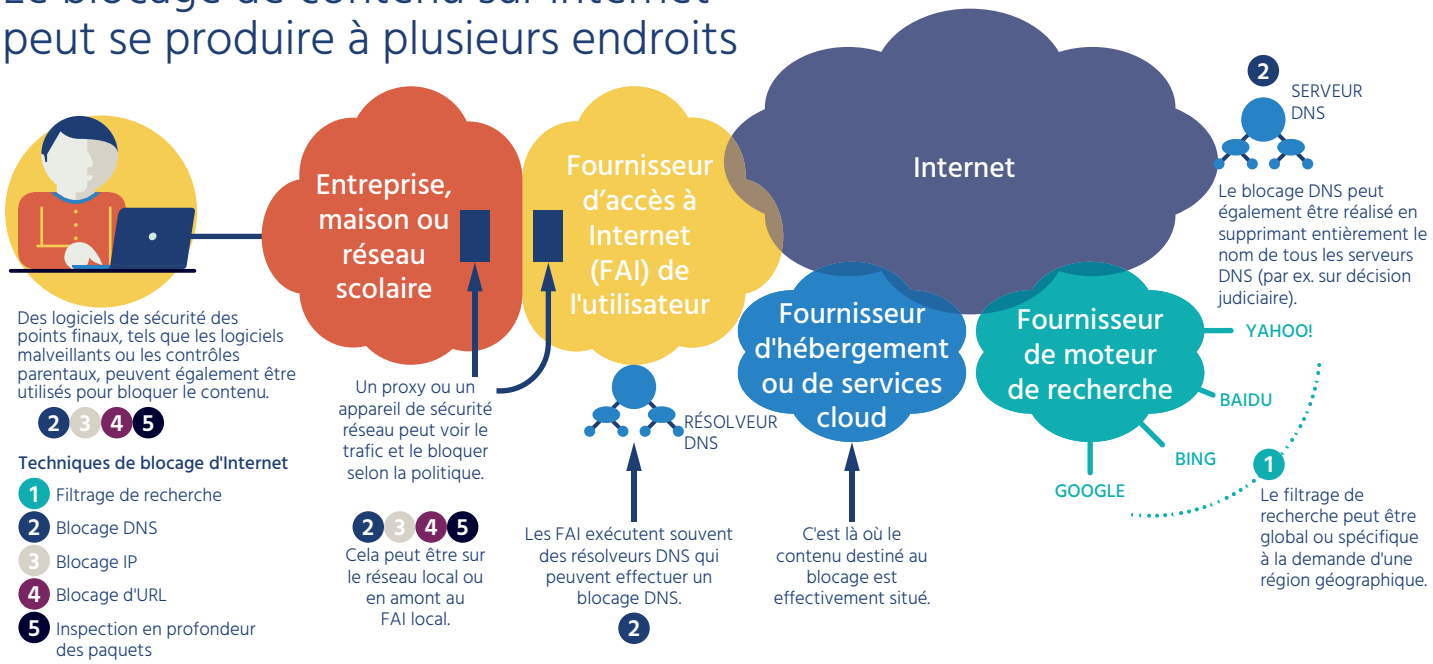
Beaucoup de techniques de blocage de contenu décrites ici peuvent être utilisées à différents endroits, comme le montre le tableau ci-dessous.

Au niveau national	Lorsqu'une politique gouvernementale l'exige, tout trafic entrant ou sortant d'un pays peut être soumis à un blocage de contenu. Cela nécessite un contrôle strict de toutes les connexions transfrontalières au moyen d'une passerelle nationale ou d'un pare-feu national, ou en parallèle pourrait être imposé à tous les opérateurs et fournisseurs d'accès à Internet (FAI) dans un pays.
Au niveau opérateur et FAI	Les entreprises de télécommunications individuelles, y compris les opérateurs de téléphonie mobile et les FAI traditionnels, peuvent installer des outils de blocage.
Au niveau d'un réseau local	Les ordinateurs portables et les périphériques de bureau d'utilisateurs finaux sont généralement connectés à des réseaux domestiques, corporatifs ou scolaires plutôt que directement à un opérateur. Ces réseaux locaux peuvent avoir installé un blocage, généralement dans l'optique d'une gestion du réseau ou de sa sécurité, plutôt que sur la base d'une politique gouvernementale.
Au niveau des points finaux	Les logiciels peuvent être installés directement sur les ordinateurs des utilisateurs qui appliquent une règle de blocage. Ceci est très fréquent dans les réseaux domestiques et d'entreprise, généralement pour des raisons de sécurité, mais aussi pour des raisons de gestion de réseau ou de contrôle parental.

Notez que, en cas de blocage basé sur des considérations de politiques publiques, la majorité des mesures sont appliquées aux deux premiers niveaux (niveau national, opérateur et FAI).

Le schéma ci-dessous résume certains des principaux endroits où le blocage peut se produire et quels types de blocage peuvent survenir à chaque point.

Le blocage de contenu sur Internet peut se produire à plusieurs endroits



Encadré :
Blocage de contenu des points finaux

Cet article se concentre sur le blocage de contenu Internet en fonction des considérations d'ordre public.

Pourtant, il est important de noter que l'un des moyens les plus efficaces de bloquer le contenu indésirable est l'utilisation de logiciels installés sur l'appareil de l'utilisateur, communément appelé « point final » car c'est le dernier point de connexion entre l'utilisateur et l'Internet. La plupart des utilisateurs d'ordinateurs utilisent un logiciel de point final pour bloquer les logiciels malveillants (virus, chevaux de Troie et phishing), qu'ils soient installés personnellement ou par un groupe informatique organisationnel.

Le logiciel de blocage de contenu de point final est également utilisé par les organisations pour bloquer le contenu pour d'autres raisons. Par exemple, les bibliothèques installent souvent ce type de logiciel sur les ordinateurs publics pour bloquer l'accès à la pornographie aux lecteurs et les parents peuvent l'utiliser pour bloquer l'accès au contenu indésirable à leurs enfants.

Le blocage de contenu des points finaux peut utiliser plusieurs des techniques décrites dans cet article, y compris la numérisation de contenu, la catégorisation d'URL, le blocage d'adresse IP et l'interception DNS. Généralement, le blocage et l'analyse se produisent sur le point final. Cependant, les fournisseurs de ce logiciel augmentent également en utilisant des outils basés sur le cloud, y compris la numérisation de contenu et le blocage DNS, en coopération avec une petite quantité de logiciels de point final. Dans ces solutions plus récentes, certains ou tous les contenus Internet peuvent passer par un service basé sur le cloud. L'avantage de déplacer la prise de décision vers le cloud est que les points finaux ne doivent pas être constamment mis à jour, et l'impact sur la performance de l'évaluation du contenu est transféré de l'ordinateur ou du téléphone intelligent de l'utilisateur vers un nuage d'ordinateurs à grande échelle. Toutefois, lorsque le trafic est acheminé par un tiers, cela crée également des problèmes de confidentialité en mettant le contenu à la disposition du tiers et, s'il est mal mis en œuvre, des problèmes de sécurité se posent également.

Evaluation des différents types de blocage

Les cinq types de blocage de contenu courants se distinguent par ce qu'ils bloquent et comment ils fonctionnent.

Ci-dessous, les techniques de blocage de contenu sont discutées plus en détail et évaluées en fonction de quatre critères spécifiques[3].

1. **Quels ensembles d'utilisateurs et de services Internet sont concernés** par cette technique ? Quels ensembles ne sont pas concernés ?

2. **Quelle est la précision** de la technique pour empêcher l'accès à un contenu particulier ? Combien de dégâts collatéraux (blocage involontaire) sont créés par cette technique de blocage ?

3. **Quelle est l'efficacité** de cette technique de blocage de contenu ? Quels types d'utilisateurs et fournisseurs de contenu peuvent contourner cette technique ?

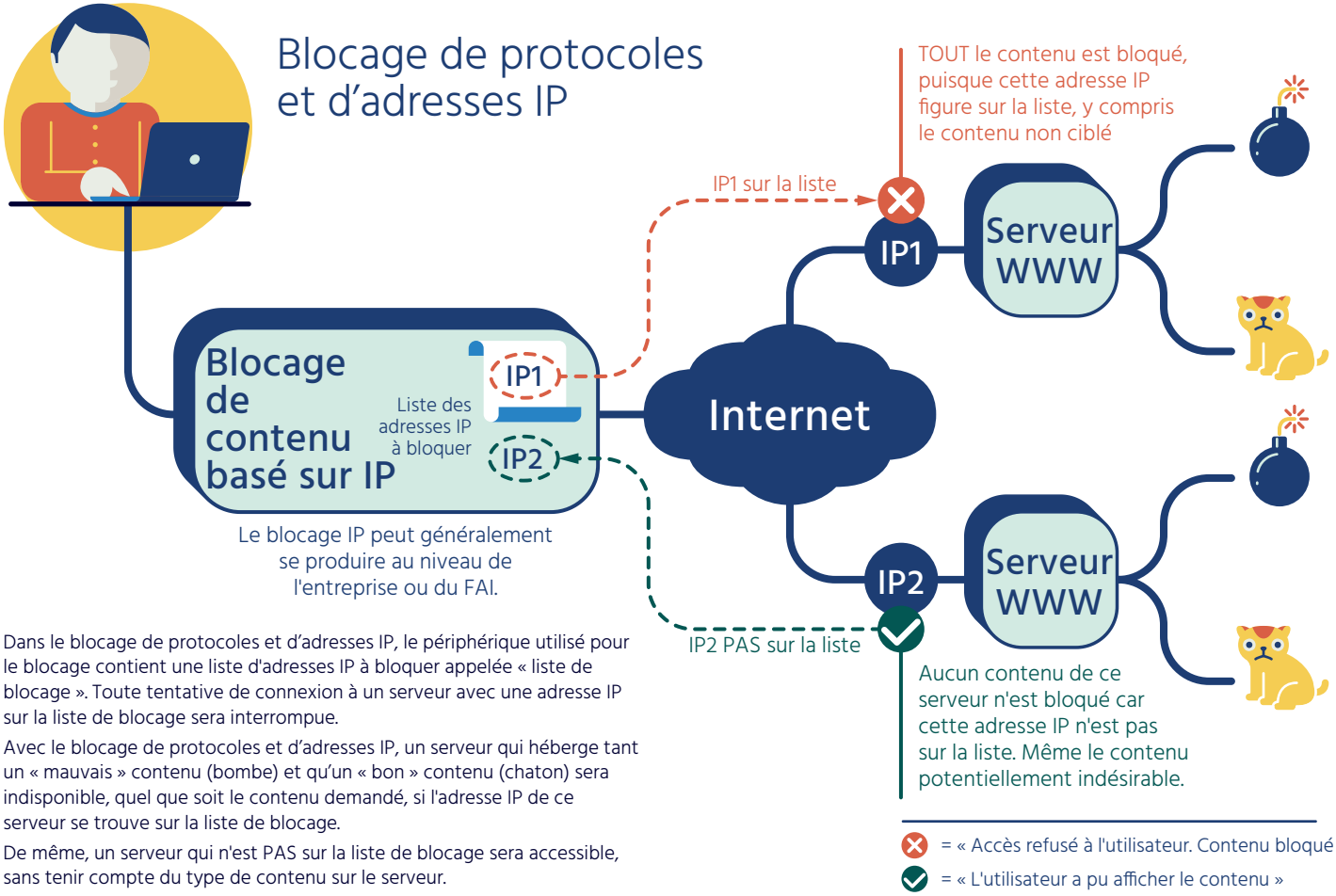
4. **Quels sont les effets secondaires courants** de cette technique ? Quels sont les problèmes techniques causés par cette technique ? Quels problèmes non techniques, tels que l'impact sur la confiance et les droits fondamentaux, sont soulevés par l'utilisation de cette technique ?

3 Ces critères sont tirés de la RFC 7754, « Considérations techniques pour le blocage et le filtrage du service Internet » :

Blocage de protocoles et d'adresses IP

Le blocage IP place des obstacles dans le réseau, tels que les pare-feux, qui bloquent tout le trafic vers un ensemble d'adresses IP. Le blocage de protocoles utilise d'autres identifiants de réseau de bas niveau, tels qu'un numéro de port TCP/IP qui peut identifier une application particulière sur un serveur ou un type de protocole d'application. Ces méthodes de blocage ne bloquent pas directement le contenu : elles bloquent le trafic vers des adresses IP connues ou des ports ou protocoles TCP/IP associés à un contenu ou une application. Le blocage de protocoles et d'adresses IP peut également être effectué par un logiciel sur les ordinateurs des utilisateurs, généralement pour des raisons de sécurité réseau.

Par exemple, si l'objectif était de bloquer tout le contenu hébergé dans le pays imaginaire d'Elbonia, le blocage IP pourrait être utilisé si l'ensemble de toutes les adresses IP hébergeant le contenu d'Elbonia était connu. De même, si l'objectif était de bloquer tous les services VPN (qui sont utilisés pour chiffrer le trafic et cacher à la fois la destination et le contenu), le blocage des protocoles pourrait être utilisé pour arrêter les services VPN en utilisant des protocoles bien connus ou des numéros de port TCP/IP.



Dans le blocage de protocoles et d'adresses IP, le périphérique utilisé pour le blocage contient une liste d'adresses IP à bloquer appelée « liste de blocage ». Toute tentative de connexion à un serveur avec une adresse IP sur la liste de blocage sera interrompue.

Avec le blocage de protocoles et d'adresses IP, un serveur qui héberge tant un « mauvais » contenu (bombe) et qu'un « bon » contenu (chaton) sera indisponible, quel que soit le contenu demandé, si l'adresse IP de ce serveur se trouve sur la liste de blocage.

De même, un serveur qui n'est PAS sur la liste de blocage sera accessible, sans tenir compte du type de contenu sur le serveur.

Une variante du blocage IP est la limitation de bande passante. Dans ce scénario, tout le trafic n'est pas bloqué, seulement un certain pourcentage. Les utilisateurs peuvent percevoir le service comme très lent, ou tout simplement fluctuant. Cela peut être utilisé pour décourager les utilisateurs d'utiliser un service en le rendant peu fiable ou encourager l'utilisation de services alternatifs, sans révéler qu'il y a un blocage. (Cela peut également être fait pour des raisons de gestion du réseau et de la bande passante à la fois au niveau du FAI ou de l'entreprise.)

Le blocage de protocoles et d'adresses IP utilise des périphériques qui se trouvent entre l'utilisateur final et le contenu, ce qui nécessite que l'entité qui effectue le blocage (tel que le FAI de l'utilisateur) ait un contrôle total sur la connexion entre l'utilisateur final et Internet. Un utilisateur qui n'est pas « derrière » le périphérique de blocage, ou qui utilise une technologie telle qu'un VPN qui cache la véritable destination de son trafic, ne sera pas affecté par ce type de blocage.

En général, le blocage IP est une technique de filtrage qui n'est pas très efficace, est difficile à maintenir, a un niveau élevé de blocage excessif involontaire et est facilement contourné par les éditeurs qui déplacent le contenu vers de nouveaux serveurs (avec de nouvelles adresses IP).

Le blocage IP ne fonctionne pas non plus lorsque les fournisseurs d'informations utilisent des réseaux de diffusion de contenu (Content Delivery Networks, CDN), car les adresses IP de l'information sont très dynamiques et changent constamment.[4] Les CDN utilisent également la même adresse IP pour de nombreux clients et types de contenu différents, ce qui entraîne un niveau élevé d'interruption involontaire du service.

Le blocage de protocoles et d'adresses IP fonctionne mieux lorsqu'il est utilisé pour bloquer des applications spécifiques plutôt que des contenus spécifiques. Par exemple, le trafic VPN peut être bloqué par les blocs de protocoles et ports TCP/IP, combinés à des blocs d'adresses IP de services publics VPN connus. C'est une technique courante et très efficace.

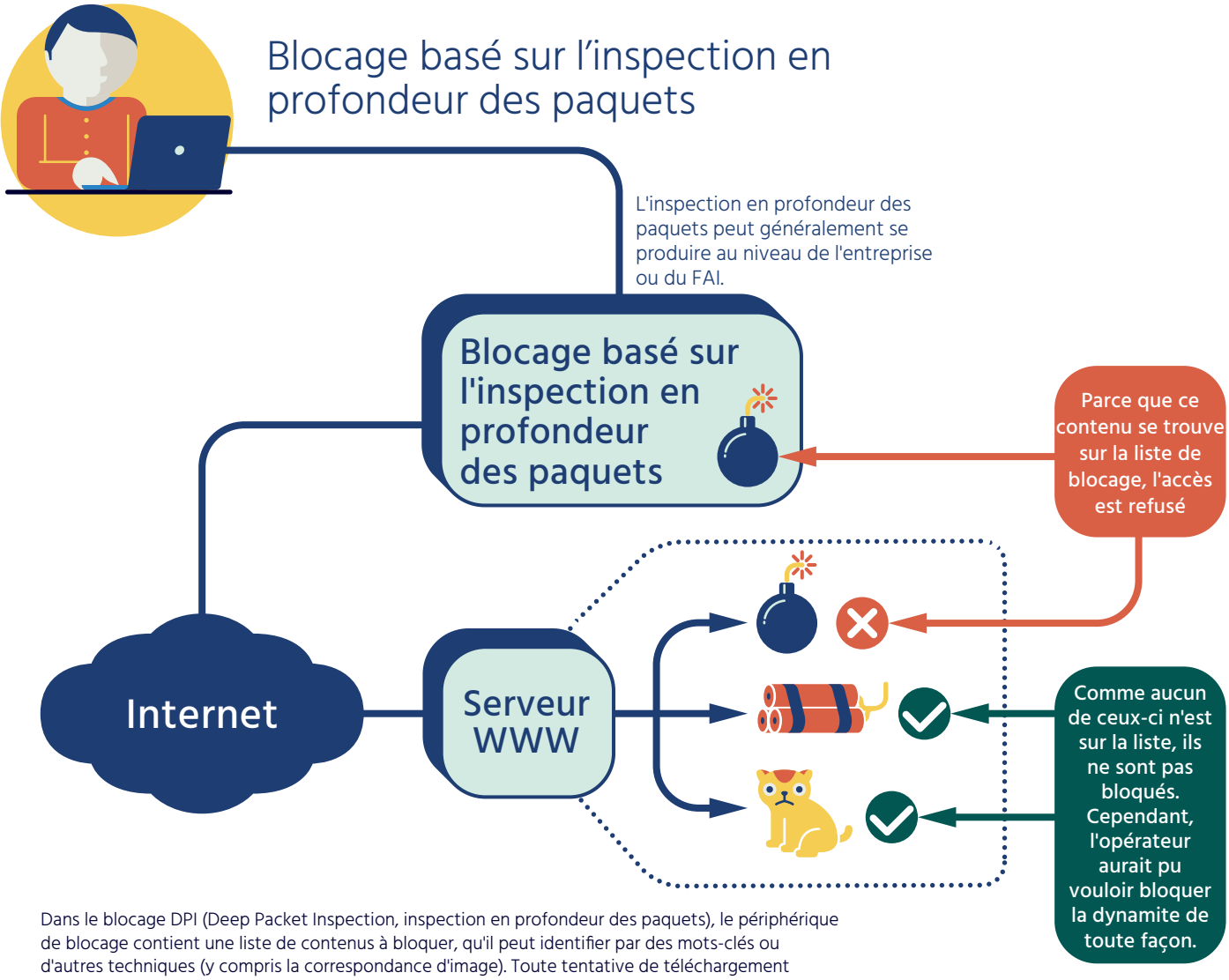
Le blocage IP est également plus efficace lorsque le contenu est hébergé dans un serveur particulier dans un centre de données spécifique, ou si un ensemble très spécifique de fichiers est ciblé. Le blocage IP n'est pas très efficace pour les services d'hébergement plus importants répartis dans de nombreux centres de données ou qui utilisent des réseaux de diffusion de contenu (CDN) pour accélérer l'accès.

4 Un réseau de diffusion de contenu est un vaste réseau réparti géographiquement de serveurs qui accélèrent la livraison du contenu Web aux internautes. Les grands CDN ont des centaines de milliers de serveurs dans de nombreux pays pour fournir un accès plus rapide au contenu de leurs clients. Les CDN stockent des copies des contenus de texte, d'image, audio et vidéo de leurs clients dans leurs propres serveurs autour des « bords » d'Internet afin que les demandes d'utilisateurs puissent être diffusées par un serveur périphérique CDN proche plutôt que par les serveurs centralisés des clients.

Blocage basé sur l'inspection en profondeur des paquets

Le blocage DPI utilise des périphériques entre l'utilisateur final et le reste de l'Internet, qui filtrent en fonction de contenus, de modèles ou de types d'applications spécifiques. Ce type de blocage du réseau demande une forte puissance de calcul et est donc coûteux, car tout le contenu doit être évalué en fonction des règles de blocage. Le blocage DPI peut également être effectué par un logiciel sur les ordinateurs des utilisateurs, généralement pour des raisons de sécurité réseau.

Le blocage DPI requiert un type de signature ou une information sur le contenu pour être efficace. Il peut s'agir de mots-clés, de caractéristiques de trafic (telles que les tailles de paquets ou les taux de transmission), de noms de fichiers ou d'autres informations spécifiques au contenu. Le blocage DPI est utilisé de manière très efficace pour bloquer ou ralentir certaines applications (telles que le partage de fichiers en pair à pair ou le trafic Voix sur IP [VoIP]) et des types de fichiers de données (tels que les fichiers multimédia).



Dans le blocage DPI (Deep Packet Inspection, inspection en profondeur des paquets), le périphérique de blocage contient une liste de contenus à bloquer, qu'il peut identifier par des mots-clés ou d'autres techniques (y compris la correspondance d'image). Toute tentative de téléchargement de contenu non chiffré qui correspond à la liste sera interrompue.

Avec DPI, les faux positifs (bloquant le contenu de manière incorrecte) et les faux négatifs (ne bloquant pas le contenu ciblé) sont courants. La DPI est également difficile à appliquer correctement lorsque le trafic est chiffré.

Dans le schéma ci-dessus, la bombe a été bloquée car elle correspond au contenu. Cependant, la dynamite n'a pas été bloquée, même si l'opérateur du périphérique DPI voulait la bloquer, car la dynamite ne correspondait pas à la liste de blocage de contenu.

Le blocage DPI est très utilisé dans les entreprises pour les systèmes de protection contre les fuites de données, les produits anti-spam et anti-logiciels malveillants (antivirus) et la régulation des flux sur le réseau (comme par exemple mettre en priorité la vidéoconférence d'entreprise). Cependant, il peut également être utilisé à des fins de blocage basé sur les politiques publiques. Par exemple, l'utilisation des services VoIP non fournis par l'opérateur national de télécommunications est souvent réglementée ou restreinte, et le blocage DPI est efficace pour faire respecter ces restrictions.

Le blocage DPI utilise des périphériques qui peuvent voir et contrôler tout le trafic entre l'utilisateur final et le contenu, de sorte que l'entité qui effectue le blocage (comme le FAI de l'utilisateur) doit avoir un contrôle total sur la connexion de l'utilisateur à Internet. Lorsque le trafic est chiffré, comme c'est souvent le cas, les systèmes de blocage DPI peuvent ne plus être efficaces. Ceux-ci sont discutés plus en détail dans l'encadré « Chiffrement, proxies et défis du blocage » à droite.

Le blocage DPI est généralement une technique efficace pour bloquer certains types de contenu qui peuvent être identifiés à l'aide de signatures ou d'autres règles (telles que « bloquer tout le trafic VoIP »). Le blocage DPI a beaucoup moins de succès avec d'autres types de contenu, tels que les fichiers multimédias particuliers ou les documents avec des mots-clés particuliers. Étant donné que le blocage DPI examine tout le trafic vers les utilisateurs finaux, il est également très envahissant dans la vie privée des utilisateurs.

L'efficacité globale du blocage DPI varie largement en fonction des buts et des outils DPI spécifiques utilisés. Généralement, les outils DPI sont les plus efficaces dans la gestion et sécurité du réseau, et ne sont pas adaptés au blocage fondé sur les politiques publiques.

Encadré :
Chiffrements, proxies et défis du blocage

Plusieurs des techniques abordées dans cet article, y compris le blocage DPI et le blocage d'URL, ont une limitation très réelle : elles doivent pouvoir voir le trafic évalué. Les serveurs Web qui offrent un chiffrement ou les utilisateurs qui ajoutent un chiffrement à leurs communications (généralement via une technologie de chiffrement spécifique à l'application, comme TLS/SSL) ne peuvent pas être bloqués de manière fiable par des périphériques réseau. Beaucoup d'autres techniques sont également facilement déjouées lorsque l'utilisateur a accès à la technologie VPN qui chiffre les communications et masque la vraie destination et le type de trafic. Bien que les chercheurs et les fournisseurs aient développé quelques façons d'identifier certains types de trafic par inférence et analyse, ces techniques ne font que deviner le type de trafic qu'elles voient.

Une recherche récente a révélé que 49 % du trafic Web des États-Unis était chiffré (en volume) en février 2016. (Voir : http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf) Ce trafic serait effectivement invisible au blocage d'URL et aux outils DPI qui examinent le contenu, car la seule information visible serait le nom de domaine du serveur hébergeant l'information. Pour compenser cette « évasion » du contentu, certains blocages de réseau utilisent des périphériques actifs (appelés proxies) qui interceptent et déchiffrent le trafic entre l'utilisateur et le serveur Web, rompant le modèle de chiffrement de bout en bout de TLS/SSL.

Lorsque des proxies sont utilisés, ils causent d'importants problèmes de sécurité et de confidentialité. En cas de rupture du modèle TLS/SSL, l'entité qui bloque accède à toutes les données chiffrées et peut permettre par inadvertance à d'autres tiers de faire la même chose. Le proxy peut également modifier le contenu. Si l'entité qui bloque a le contrôle du système de l'utilisateur (par exemple, un périphérique géré par l'entreprise), le proxy peut être très transparent. Généralement, cependant, la présence d'un proxy devrait être visible par l'utilisateur final, du moins pour le trafic crypté (TLS/SSL) (p. ex. l'utilisateur peut obtenir une alerte indiquant que le certificat ne provient pas d'une autorité de confiance). En outre, les nouvelles normes de l'industrie et de l'IETF (telles que HTTP Strict Transport Security [RFC6797], HTTP Public Key Pinning [RFC 7469] et DANE [RFC 6698]) et de nouvelles fonctionnalités de sécurité dans les navigateurs Internet modernes compliquent le fait de substituer (et décrypter) le trafic TLS/SSL sans que l'utilisateur final le sache et coopère.

Les proxies installés pour des raisons de blocage de contenu peuvent également créer des goulots d'étranglement de performance dans le flux de trafic réseau, rendant les services lents ou peu fiables.

Blocage d'URL

Le blocage d'URL est une méthode de blocage très populaire et peut se produire à la fois sur un ordinateur individuel ou sur un périphérique réseau entre l'ordinateur et le reste de l'Internet. Le blocage d'URL fonctionne avec des applications Web et n'est pas utilisé pour bloquer des applications non Web (telles que VoIP). Avec le blocage d'URL, un filtre intercepte le flux du trafic Web (HTTP) et vérifie l'URL, qui apparaît dans la requête HTTP, par rapport à une base de données locale ou un service en ligne. Selon la réponse, le filtre URL autorisera ou bloquera la connexion au serveur Web demandé.

Généralement, les URL sont gérées par catégorie (par exemple, « sites sportifs ») et une catégorie entière est bloquée, ralentie ou autorisée.[5] Dans le cas d'une politique nationale requérant un blocage d'URL, la politique de de blocage de contenu est souvent gérée par le gouvernement. Le filtre URL peut simplement arrêter le trafic, ou il peut rediriger l'utilisateur sur une autre page Web, affichant les raisons du blocage ou mentionnant simplement que le trafic a été bloqué. Le blocage d'URL dans le réseau peut être appliqué par des proxies, ainsi que par des pare-feu et des routeurs.

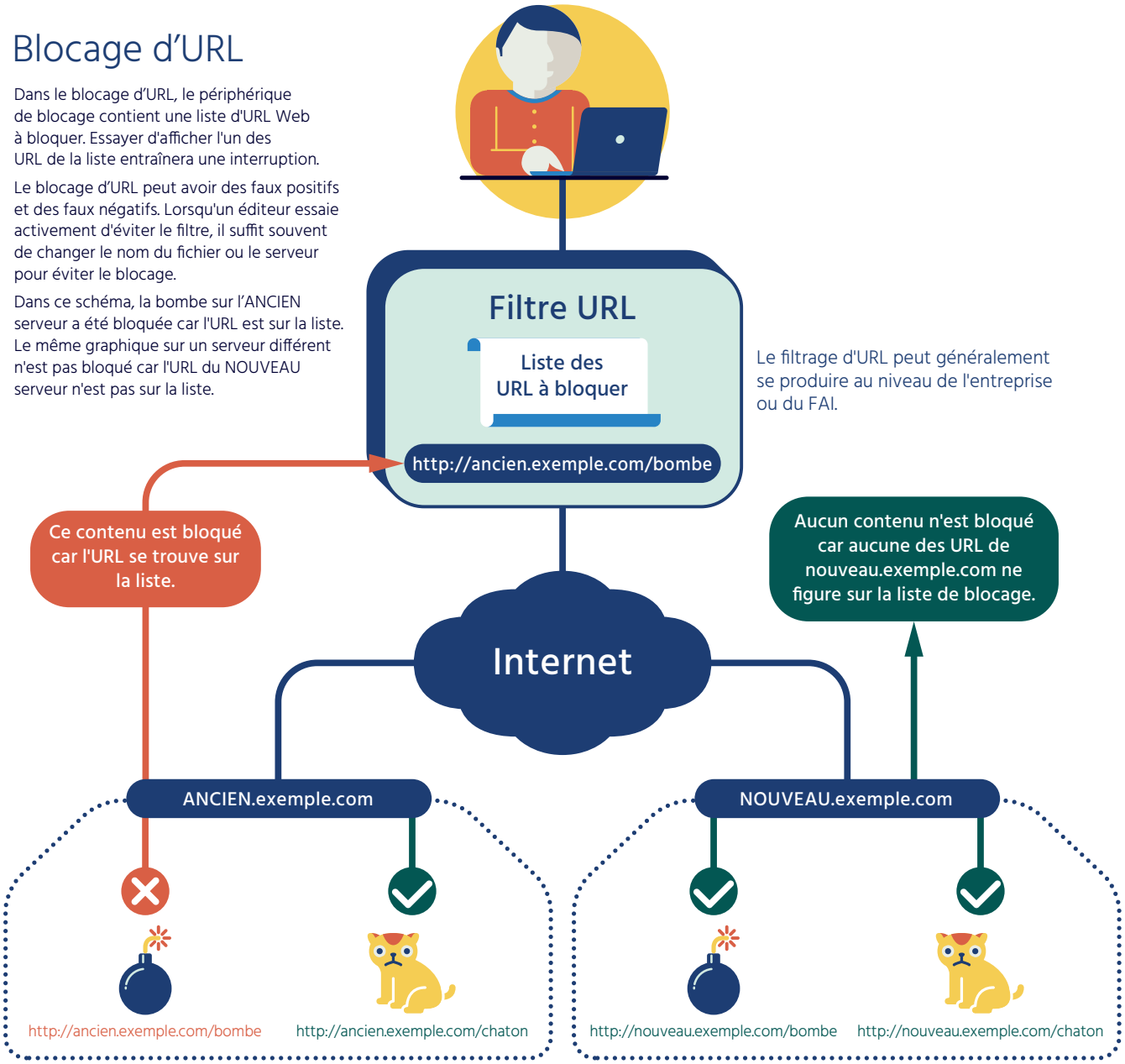
5 Les catégories de filtrage d'URL sont établies par les fournisseurs de services de sécurité et sont souvent basées sur une combinaison d'analyses humaines de pages Web associées à une analyse automatisée du contenu de la page Web. La plupart des fournisseurs de services de sécurité offrent des bases de données de filtrage d'URL pour la gestion du trafic réseau d'entreprise, mais elles peuvent être utilisées dans d'autres contextes, comme ceux décrits dans cet article.

Blocage d'URL

Dans le blocage d'URL, le périphérique de blocage contient une liste d'URL Web à bloquer. Essayer d'afficher l'un des URL de la liste entraînera une interruption.

Le blocage d'URL peut avoir des faux positifs et des faux négatifs. Lorsqu'un éditeur essaie activement d'éviter le filtre, il suffit souvent de changer le nom du fichier ou le serveur pour éviter le blocage.

Dans ce schéma, la bombe sur l'ANCIEN serveur a été bloquée car l'URL est sur la liste. Le même graphique sur un serveur différent n'est pas bloqué car l'URL du NOUVEAU serveur n'est pas sur la liste.



Le blocage d'URL nécessite que l'entité qui effectue le blocage (tel que le FAI de l'utilisateur) ait la possibilité d'intercepter et de contrôler le trafic entre l'utilisateur final et Internet. Le blocage d'URL est habituellement coûteux, car le périphérique de filtrage doit généralement être en ligne entre l'utilisateur et Internet, et nécessite donc un haut niveau de ressources pour donner des performances acceptables.

Le blocage d'URL est généralement considéré comme très efficace pour identifier le contenu qui peut être sur différents serveurs ou services car l'URL ne change pas même si le serveur modifie ses adresses IP. Dans quelques cas, le blocage d'URL risque de ne pas bloquer complètement le trafic lorsque les URL sont très compliquées ou changent fréquemment. Cela peut se produire car un éditeur d'informations a délibérément décidé d'échapper au blocage des filtres URL, ou il peut s'agir d'un effet secondaire de certains systèmes de publication avancés tels que ceux utilisés pour les grandes publications en ligne.

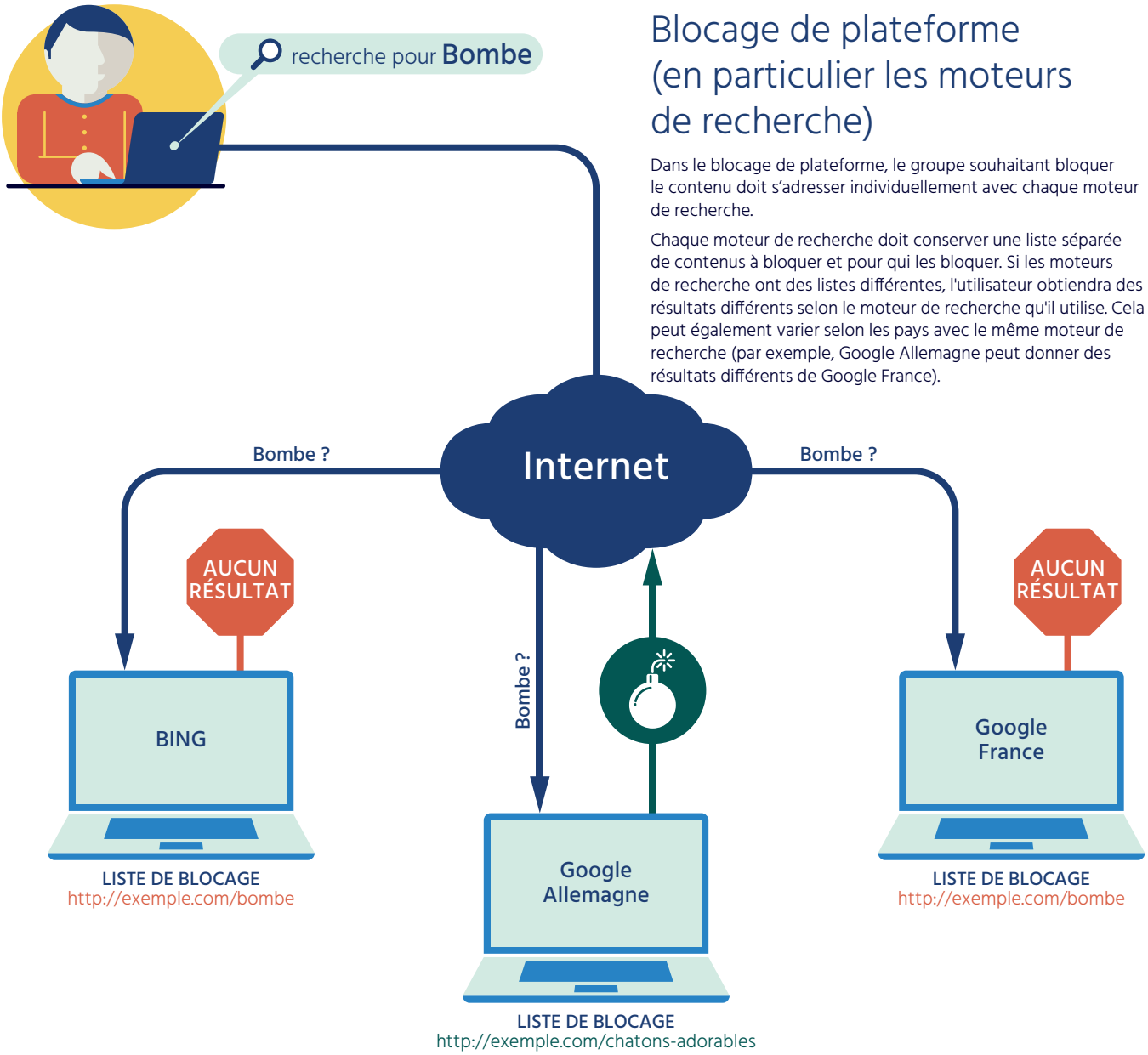
Le blocage d'URL est habituellement efficace sur les URL de haut niveau, comme une page Web particulière, mais n'est pas aussi efficace lorsque des liens profonds (tels que des éléments de contenu individuels dans une page Web) sont considérés. Selon la façon dont l'utilisateur a navigué vers le contenu particulier, le blocage d'URL peut ou non bloquer tout accès - si l'utilisateur a un « lien profond » non couvert par le filtre URL, le contenu sera autorisé. Par exemple, le site Web de Playboy inclut les URL playboy.com, mais aussi le contenu intégré utilisant le nom de domaine « playboy.tv ». Un filtre URL n'incluant pas non plus les URL « playboy.tv » ne bloquerait pas le contenu vidéo.

Tous les types de blocage d'URL dépendent fortement de la qualité du filtre, et un filtre mal conçu ou trop général peut bloquer du trafic non ciblé ou avoir d'autres effets négatifs sur l'expérience de l'utilisateur, par exemple en affectant le chargement ou le formatage des pages Web lorsqu'un composant est bloqué.

Comme pour les blocages DPI, le blocage d'URL requiert un certain type de proxy pour voir l'URL complète lorsque le trafic est chiffré avec HTTPS (TLS/SSL). Voir l'encadré « Chiffrement, proxies et défis du blocage », page 15, pour plus d'informations sur les effets sur la vie privée des utilisateurs. Pour le trafic chiffré, le blocage d'URL ne permet de voir que l'adresse IP du serveur et non l'URL complète, ce qui entraîne un niveau beaucoup plus élevé de blocage involontaire. Étant donné que les proxies sont coûteux et intrusifs pour l'expérience de l'utilisateur, le blocage d'URL ne fonctionne pas bien comme un outil pour le blocage basé sur des politiques publiques.

Blocage de plateforme (en particulier les moteurs de recherche)

Dans certains cas, les autorités nationales travailleront avec les principales plateformes de contenu pour bloquer des informations dans leur région géographique sans bloquer toute la plateforme. Les exemples les plus courants de filtrage de plateformes sont les principaux fournisseurs de moteurs de recherche et les plateformes de réseaux sociaux. Récemment, il a également été signalé que les magasins d'applications mobiles (tels que Apple Store et Google Play) travaillent avec les autorités nationales pour bloquer les téléchargements d'applications spécifiques dans leur pays.



Le blocage de plateforme est une technique qui nécessite l'assistance du propriétaire de la plateforme, tel qu'un opérateur de moteur de recherche comme Google ou Microsoft. Dans cette technique, les requêtes d'un ensemble particulier d'internautes vers un moteur de recherche recevront un ensemble de résultats différents du reste de l'Internet, filtrant les pointeurs vers des contenus qui, d'une manière ou d'une autre, ont été considérés comme répréhensibles. Dans certains cas, la définition de ce qui doit être bloqué est basée sur la réglementation locale et les exigences gouvernementales, mais cela peut aussi être dû aux politiques internes de l'opérateur du moteur de recherche. Par exemple, un moteur de recherche peut bloquer les pointeurs vers des logiciels malveillants ou un contenu jugé inapproprié en fonction de ses propres termes de service.

Parce que le blocage des moteurs de recherche requiert la coopération du fournisseur de moteur de recherche, cela limite son utilisation à deux scénarios très spécifiques : règles au niveau du pays (blocage du contenu basé sur des règles propres à chaque pays ou région) et règles basées sur l'âge (blocage du contenu inapproprié pour les jeunes).

Le blocage des moteurs de recherche affecte uniquement les utilisateurs qui choisissent un moteur de recherche particulier, et seulement lorsque les utilisateurs sont identifiés comme appartenant à un ensemble particulier avec des règles de filtrage. Dans le blocage basé sur l'âge, comme SafeSearch[6] (proposé par les principaux moteurs de recherche et fournisseurs de contenu), un opt-in explicite est nécessaire.

Étant donné que le blocage des moteurs de recherche ne filtre que les pointeurs vers le contenu et non le contenu lui-même, il s'agit d'une technique extrêmement inefficace et qui peut avoir la conséquence involontaire d'attirer l'attention sur le contenu bloqué. La présence de moteurs de recherche multiples, ainsi que d'autres méthodes de recherche de contenu, rendent ce type de blocage très difficile à appliquer.

Bien que le blocage des moteurs de recherche semble être très peu utilisé pour bloquer le contenu, la technique est extrêmement populaire au niveau national et les gouvernements du monde entier exigent que les principaux moteurs de recherche mettent en œuvre des filtres en fonction de leur réglementation, comme la violation du droit d'auteur ou des types de discours particuliers interdits par la législation nationale. Par exemple, Google a signalé en 2015 avoir reçu 8398 demandes de 74 juridictions nationales pour supprimer 36834 résultats de ses résultats de recherche.[7] Les demandes de particuliers concernant la violation du droit d'auteur sont également très populaires : en juin 2016, Google a déclaré que 6937 propriétaires de droits d'auteur avaient demandé que plus de 86 millions de résultats de recherche soient supprimés des résultats de Google au cours de ce même mois.[8]

Le blocage des moteurs de recherche est également utilisé par les particuliers dans le cadre du « droit à l'oubli », avec plus d'un million d'URL internationalement demandées à être bloquées au cours des deux dernières années (mai 2014 à juin 2016).

Encadré :
Blocage sur d'autres plateformes

Bien que le blocage des moteurs de recherche soit le type le plus courant de blocage de plateforme, d'autres plateformes avec d'énormes communautés d'utilisateurs sont souvent prises en compte pour cette technique. Des exemples courants de ces types de plateformes incluent Facebook (qui compte plus de 1,5 milliard d'utilisateurs actifs chaque mois) et YouTube (avec plus d'un milliard d'utilisateurs uniques). Les tentatives d'utilisation de techniques basées sur le réseau ou basées sur des URL pour bloquer des éléments de contenu individuels, comme un article d'informations particulier, sont très difficiles. Pour ne pas devoir bloquer tout un site (Facebook, par exemple), les autorités nationales ont proposé de travailler avec les principaux fournisseurs de plateformes pour filtrer les types spécifiques de contenu qu'elles jugent illégal.

On connaît très peu sur l'efficacité, la portée ou les effets secondaires d'autres types de blocage de plateforme, car cette technique n'a pas été largement et fiablement observée sur des plateformes autres que les moteurs de recherche Bien que les principales plateformes, telles que Facebook, YouTube et Twitter, bloquent universellement certains types de contenu (comme les logiciels malveillants et le matériel pornographique) et fournissent des flux de contenu personnalisés à leurs utilisateurs, les informations sur les blocages spécifiques ne sont pas disponibles.

6 SafeSearch est une fonctionnalité des principaux moteurs de recherche, y compris Google Search, Microsoft Bing et Yahoo !, qui bloque les résultats contenant des « images inappropriées ou explicites » à partir des résultats de recherche.

7 https://www.google.com/transparencyreport/removals/government/?hl=en

8 https://www.google.com/transparencyreport/removals/copyright/?hl=en

Blocage de contenu au niveau du DNS

Le blocage de contenu au niveau du DNS évite l'un des problèmes rencontrés avec d'autres techniques : l'impact sur le coût et la performance lors du filtrage de tout le trafic réseau. Au lieu de cela, le blocage de contenu au niveau du DNS se concentre sur l'examen et le contrôle des requêtes DNS.

Avec le blocage de contenu au niveau du DNS, un résolveur DNS spécialisé (voir l'encadré : Vue d'ensemble du DNS) a deux fonctions : en plus d'effectuer des recherches DNS, le résolveur vérifie les noms sur une liste de blocage. Lorsque l'ordinateur d'un utilisateur essaie d'utiliser un nom bloqué, le serveur spécial renvoie des informations incorrectes, telles que l'adresse IP d'un serveur affichant un avis indiquant que le contenu a été bloqué. Ou, le serveur peut prétendre que le nom n'existe pas. Le résultat est que l'utilisateur est empêché d'accéder facilement au contenu en utilisant certains noms de domaine.

Comme pour tous les blocages réseau, le blocage de contenu au niveau du DNS n'est efficace que lorsque l'organisation qui effectue le blocage a un contrôle total sur la connexion réseau de l'utilisateur final. Si l'utilisateur peut sélectionner une connexion différente ou utiliser un ensemble différent de serveurs DNS, la technique ne l'affecte pas. Par exemple, lorsque la Turquie a bloqué certaines requêtes DNS en 2012, les utilisateurs ont changé leurs systèmes pour utiliser les serveurs DNS publics de Google et éviter le blocage. Les autorités turques ont réagi en détournant tout le trafic vers le service DNS de Google, ce qui a causé des dommages collatéraux importants. Le blocage de contenu au niveau du DNS nécessite des pare-feu ou d'autres périphériques pouvant intercepter et rediriger toutes les requêtes DNS vers les serveurs DNS spécialement conçus pour le blocage, sous peine de ne pas être très efficace.

L'efficacité du blocage de contenu au niveau du DNS est similaire au blocage IP. Il est légèrement plus efficace car la liste des noms de domaine est plus facile à mettre à jour et est plus précise qu'une liste d'adresses IP pour la plupart des types de blocage de contenu. Cependant, il est légèrement moins efficace car la modification des noms de domaine est plus simple que le changement d'adresses IP, ce qui permet aux utilisateurs finaux et aux plateformes d'informations de déjouer ce type de blocage.

Une autre forme de blocage de contenu au niveau du DNS est lorsque les noms de domaine sont enlevés ou supprimés du DNS. Cette méthode est plus difficile à contourner et les dommages collatéraux sont quelque peu limités. Dans de nombreux cas, cela dépend de l'efficacité de la coopération transfrontalière, lorsqu'une demande ou une ordonnance judiciaire provient d'une juridiction différente de celle d'où registre est basé.

Le blocage de contenu au niveau du DNS a des inconvénients similaires au blocage IP : tant du contenu ciblé que non-ciblé pour interdiction peut figurer sur le même serveur en utilisant le même nom (tel que « facebook.com »), et donc tout le contenu serait bloqué. En outre, la modification des réponses DNS peut provoquer d'autres problèmes techniques qui interrompent d'autres services valables.[9]

Le blocage de contenu au niveau du DNS repose également sur le scénario d'une utilisation normale du service DNS standard pour traduire les noms en adresses IP. Les utilisateurs qui ont un contrôle total sur leurs propres ordinateurs et une expertise technique peuvent les reconfigurer pour déjouer le service DNS standard et utiliser des solutions de rechange, ou simplement avoir une liste des traductions de noms vers adresses IP stockées localement.

Encadré :
Vue d'ensemble du DNS

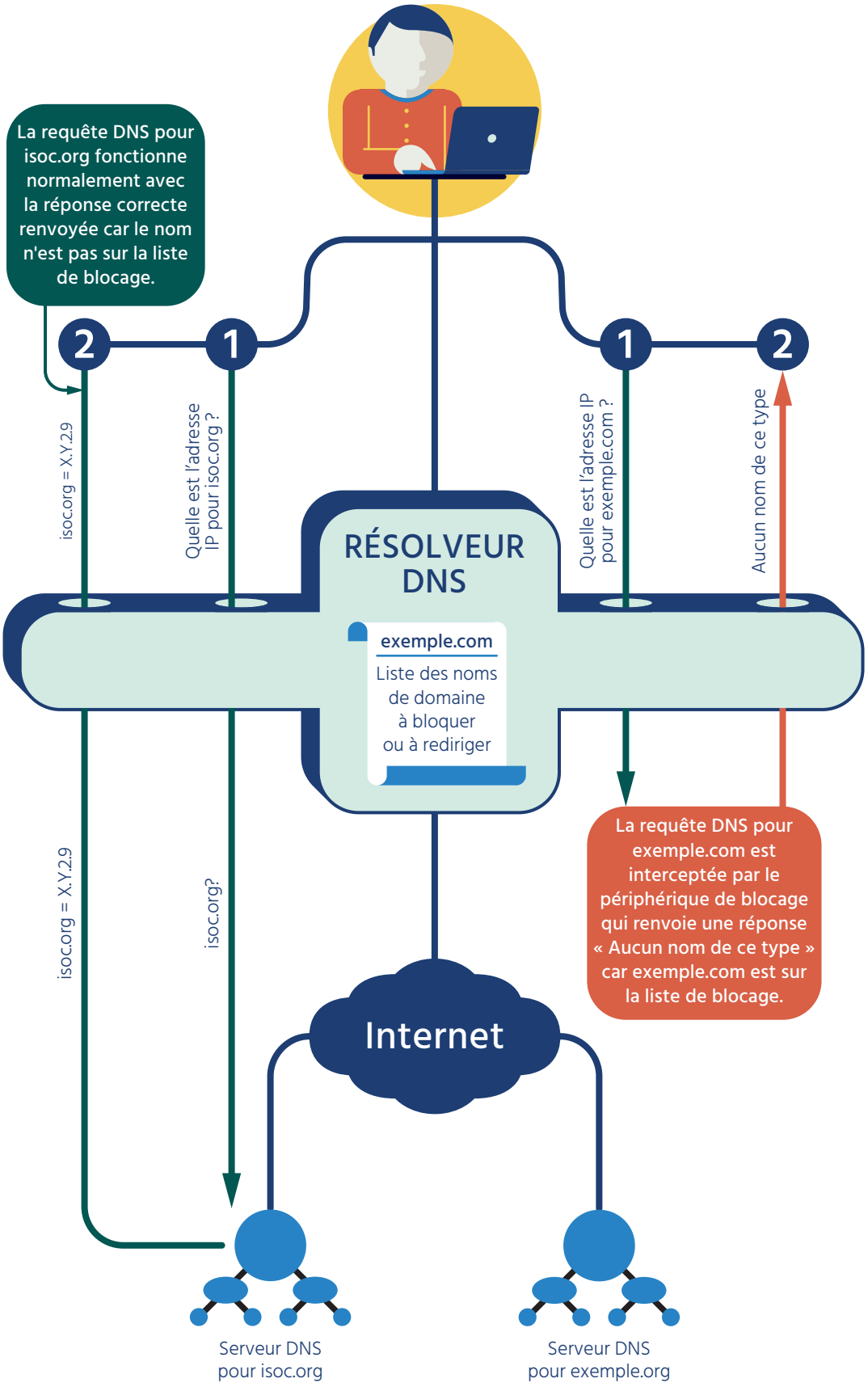
Le DNS est un système conceptuellement simple qui permet de rechercher une chaîne de labels (telles que « www », « isoc » et « org ») séparées par des points (le nom de domaine) dans une base de données répartie sur plusieurs serveurs DNS La recherche de nom de domaine aboutit à une réponse (par exemple, une adresse IP ou un site Web), ou à la réponse que le nom n'existe pas.

Le type de recherche DNS le plus courant concerne les adresses IP (protocole Internet). Il s'agit du type de consultation qui se produit chaque fois qu'un utilisateur tape un URL dans un navigateur Web par exemple. Normalement, l'application individuelle (telle que le navigateur Web) n'effectue pas la consultation totale, qui implique plusieurs étapes. L'application a plutôt recours à un système intermédiaire appelé « résolveur » (car il résout les recherches de noms DNS), qui navigue dans la base de données distribuée du DNS afin de récupérer l'information demandée.

Dans le blocage de contenu basé sur DNS, le fonctionnement normal du résolveur est modifié.

9 Les lecteurs souhaitant en savoir plus peuvent consulter le rapport « Points de vue sur le filtrage DNS » de l'Internet Society sur https://www.internetsociety.org/internet-society-perspectives-domain-name-system-dns-filtering-0

Blocage DNS



Dans le blocage DNS, le périphérique de blocage contient une liste de noms DNS à bloquer.

Étant donné que la plupart des connexions Internet nécessitent la traduction d'un nom DNS en adresse IP, le blocage de la requête et le renvoi d'une fausse réponse peuvent empêcher les utilisateurs d'essayer de récupérer du contenu bloqué ou de se connecter à des services bloqués par d'autres moyens (p. ex. en tapant directement l'adresse IP).

Blocage de contenu : résumé

Techniques de blocage de contenu sur Internet					
	Blocage de protocoles et d'adresses IP	**Blocage basé sur l'inspection en profondeur des paquets (DPI)**	**Blocage d'URL**	**Blocage de plateforme (en particulier les moteurs de recherche)**	**Blocage DNS**
Vue d'ensemble	Un périphérique est inséré dans le réseau qui se bloque en fonction de l'adresse IP et/ou de l'application (p. ex. VPN).	Un périphérique est inséré dans le réseau qui se bloque en fonction des mots-clés et/ou d'un autre contenu (nom de fichier, par exemple).	Un périphérique est inséré dans le réseau qui intercepte les requêtes Web et recherche les URL sur une liste de blocage.	Fonctionnant avec les plateformes d'information (comme les moteurs de recherche), le contenu est modifié selon les exigences locales.	Au niveau du réseau ou du FAI, le trafic DNS est dirigévers un serveur DNS modifié qui peut bloquer les recherches de certains noms de domaine.
Est-ce efficace ?	Étant donné que les adresses IP sont facilement modifiées et que le contenu est facilement déplacé, cette technique fonctionne mal. Elle ne fonctionne que si l'éditeur d'informations ne travaille pas activement pour échapper au blocage.	Lorsque les informations bloquées sont facilement caractérisées, c'est très efficace. Pour le blocage général (p. ex. « bloquer le contenu pour adultes ») ou face au chiffrement, la technique **est très inefficace.**	C'est une technique courante qui fonctionne bien lors du blocage de l'accès à des catégories entières d'informations. De nouvelles pages et de petits sites passent facilement au travers, tout comme les serveurs Web cryptés.	Parce qu'il n'y a pas de monopole dans les moteurs de recherche (par exemple) et que les préférences des consommateurs changent constamment, ce type de blocage est en grande partie superficiel et fonctionne mal.	Le blocage DNS est facilement contourné à la fois par les éditeurs de contenu et les utilisateurs finaux. Le blocage DNS n'est efficace que lorsque chaque nom a une très faible quantité de contenu et que tout ce contenu doit être bloqué. **Les défis techniques, le blocage excessif et la facilité de contournement en font une technique inefficace.**
Qui est concerné ?	Quiconque se trouvant « derrière » le périphérique est concerné.	Quiconque se trouvant « derrière » le périphérique est concerné.	Utilisateurs « derrière » le périphérique et pour lesquels le périphérique peut intercepter et évaluer le trafic Web.	Utilisateurs du moteur de recherche qui a installé le blocage.	Utilisateurs du serveur DNS modifié. Cela peut être appliqué au niveau du réseau ou du fournisseur de services.
À quel point est-ce ciblé?	**Affecte tout le contenu sur un serveur, qu'il soit illégal ou non.** Cela fonctionne même lorsque les données sont cryptées.	**Affecte uniquement le contenu qui correspond aux règles de blocage.** Nécessite des proxies pour fonctionner avec des pages Web chiffrées.	**Affecte des pages Web et des éléments Web individuels.** Nécessite des proxies pour fonctionner avec des pages Web chiffrées.	**Affecte des pages Web et des éléments Web individuels.** Généralement effectué au niveau individuel de l'URL.	**Affecte tout contenu fourni par un nom de domaine, qu'il soit illégal ou non.** Ne peut pas être utilisé efficacement pour distribuer du contenu.
De quel type de technique s'agit-il ?	Bloque le contenu	Bloque le contenu	Bloque le contenu	Décourage et frustre l'accès	Décourage et frustre l'accès
Combien de dommages collatéraux sont causés ?	Tout ciblage de serveurs plus grands a un énorme taux de faux positif, bloquant le contenu illégal et légal.	Selon la qualité des règles de blocage, le taux de faux positif peut varier de très faible à assez élevé. Rédiger de bonnes règles est difficile.	La plupart des filtrages d'URL sont basés sur des services commerciaux qui classent le trafic. Pour les blocages classiques, cela peut être assez spécifique, mais pour les blocages spéciaux, le taux d'erreur est assez élevé.	Le taux de faux positif est considéré comme faible, car chaque blocage de page est requis individuellement. Le problème des demandes non légitimes provoque des informations inappropriées au blocage.	Tout ciblage de noms de domaine utilisés par les serveurs plus grands a un énorme taux de faux positif, bloquant à la fois le contenu illégal et légal. Inefficace lorsque les CDN sont utilisés (ou provoque un niveau extrêmement élevé de faux positifs).
Quels sont les moyens courants d'y échapper ?	Les éditeurs peuvent modifier les adresses IP, migrer du contenu ou utiliser des réseaux de diffusion de contenu (CDN) pour y échapper. Les utilisateurs VPN y échappent en cachant les adresses IP.	Plusieurs couches de cryptage permettent de déjouer efficacement ce type de blocage. Lorsque les règles de filtrage sont mal écrites, de petites modifications de texte peuvent contourner facilement les blocages.	Plusieurs couches de cryptage permettent de déjouer efficacement ce type de blocage. L'utilisation d'une couche d'application non standard est souvent une technique efficace de contournement.	Les utilisateurs peuvent choisir des plateformes alternatives, comme un moteur de recherche différent, très facilement.	Les utilisateurs peuvent éviter d'utiliser des recherches DNS en utilisant des installations locales, ou peuvent envoyer leurs requêtes à un serveur public non modifié (généralement via un VPN).
Y a-t-il des effets secondaires ou des problèmes techniques ?	Le maintien de longues listes d'adresses IP est difficile et source d'erreurs, et nécessite des ressources importantes. Les périphériques réseau utilisant ce type de blocage sont généralement rapides, de sorte que les problèmes de performances ne sont pas courants.	Le filtrage basé sur l'analyse du contenu présente des coûts de performance importants et n'est pas pratique dans de nombreux environnements (sans ressources importantes). Lorsque des proxies sont utilisés, la sécurité peut être sérieusement compromise.	Le filtrage d'URL peut provoquer des problèmes de performance, diminuant la vitesse globale et la fiabilité. Lorsque des proxies sont utilisés, la sécurité peut être sérieusement compromise.	Beaucoup de moteurs de recherche signalent des informations « supprimées », créant ainsi une piste vers le contenu.	La sécurité DNS est compromise lorsqu'un serveur modifié est déployé.

Conclusion

Comprendre les différentes techniques de blocage, leurs conséquences et effets secondaires, est important tant pour les décideurs politiques considérant l'utilisation de ces mesures, que pour les défenseurs de l'Internet et d'autres personnes souhaitant influencer les pratiques de blocage de contenu.

Toutes les techniques de blocage sont sujettes à deux inconvénients principaux :

1. **Elles ne résolvent pas le problème**

   Les techniques de blocage ne suppriment pas le contenu d'Internet, n'empêchent pas l'activité illégale et ne poursuivent pas les coupables ; elles mettent tout simplement un rideau devant le contenu. Le contenu sous-jacent reste en place.

2. **Elles infligent des dommages collatéraux**

   Toutes les techniques de blocage sont marquée par le risque de blocage excessif et de sous-blocage : bloquant plus que prévu et, en même temps, moins que prévu. Elles causent également d'autres dommages à Internet en mettant les utilisateurs en danger (car ils essaient de contourner les blocages), en réduisant la transparence et la confiance dans Internet, en encourageant les services « souterrains » et en s'immisçant dans la vie privée des utilisateurs. Ce sont des coûts dont il faut tenir compte lors des discussions sur le blocage.

Encadré :
Contourner le blocage de contenu

Les décideurs doivent garder à l'esprit un point important lorsqu'ils envisagent de bloquer le contenu sur Internet : toutes les techniques de blocage peuvent être contournées par un utilisateur suffisamment motivé. Dans de nombreux cas, seul un effort minimal est nécessaire pour échapper au blocage.

Si le trafic vers un hôte ou un nom de domaine est bloqué, des outils tels que les VPN peuvent être utilisés pour cacher le trafic. Si le contenu du trafic est inspecté, il peut être chiffré afin qu'il ne déclenche pas le blocage. Si le contenu est retiré, d'autres utilisateurs peuvent le recharger sur d'autres serveurs. Si le nom de domaine utilisé est supprimé, les utilisateurs finaux peuvent toujours accéder à l'hôte s'ils connaissent l'adresse IP, ou un nouveau nom de domaine peut être sélectionné en remplacement. Si un moteur de recherche supprime les résultats, il existe toujours d'autres moteurs de recherche.

Les utilisateurs finaux ne sont pas les seuls à pouvoir échapper aux blocs et à le faire. Les éditeurs d'informations ont également de nombreuses approches pour esquiver diverses techniques de blocage. Si un éditeur travaille assez dur pour distribuer et diffuser du contenu, aucune technique de blocage ne peut l'arrêter.

Recommandations

L'Internet Society estime que le moyen le plus approprié pour contrer les contenus et activité illicites sur Internet est de les attaquer à la source. L'utilisation de filtres pour bloquer l'accès au contenu en ligne est sans effets durables, susceptible d'être inefficace et a tendance à générer des dommages collatéraux affectant tous les internautes.

Nous proposons deux stratégies principales aux décideurs politiques préoccupés par les contenus illégaux sur Internet :

1. **Attaquer le problème à la source :** l'approche la moins dommageable pour Internet est d'attaquer les contenus et les activités illicites à leur source. L'élimination du contenu illégal à sa source et la poursuite des auteurs évitent les effets négatifs du blocage et sont plus efficaces pour éliminer le contenu illégal.[10] La coopération entre les juridictions et les parties prenantes est une condition préalable à la réussite, car les contenus illégaux en ligne dépassent les frontières nationales et le droit national.

10 Lorsque l'autorité nationale est dans la même juridiction que le consommateur de contenu, éliminer le contenu illégal à la source semble un moyen simple de contourner les complexités et ressources requises lors de mesures transfrontalières. Nous reconnaissons que l'élimination du contenu à la source est difficile dans le contexte d'un Internet transfrontalier, où les fournisseurs et les consommateurs de contenu peuvent être situés dans différentes juridictions, sujets à des lois différentes. Pourtant, nous considérons que cela ne doit pas être une raison de ne pas identifier des solutions plus efficaces ne nuisant pas à Internet.

2. **Utiliser en priorités et utiliser des approches différentes :** Selon les circonstances, l'utilisation d'approches alternatives peut être efficace. Par exemple

    - Une coopération efficace entre les fournisseurs de services, les forces de police et les autorités nationales peut fournir des moyens supplémentaires pour aider les victimes de contenu illégal et engager des poursuites contre les auteurs.[11]
    - Créer un environnement de confiance où les utilisateurs reçoivent des informations sur ce qui est légal et ce qui ne l'est pas, peut améliorer l'autorégulation.
    - Dans certains cas (p. ex. le contrôle parental), permettre aux utilisateurs d'utiliser des filtres sur leurs propres appareils, avec leur consentement, peut être efficace et moins dommageable pour Internet.
    - Sur une base volontaire ou juridique, certains sites Web (p. ex. les sites de jeu de hasard) pourraient utiliser la géolocalisation pour empêcher l'accès des pays où leurs services ne sont pas autorisés.

Minimiser les effets négatifs

Toutes les techniques de blocage de contenu présentent de sérieuses lacunes, en particulier dans le contexte du blocage basé sur des considérations de politiques publiques. Toutes les techniques fonctionnent mal et peuvent être déjouées. Pour cette raison, et pour les raisons exposées précédemment, nous déconseillons le blocage de contenu.

Néanmoins, ces techniques sont toujours utilisées. Conscients cette réalité, nous suggérons les considérations suivantes afin d'atténuer l'impact négatif de ces mesures :

a. **Avoir épuisé toutes les options alternatives au blocage :** tout d'abord, épuisez toutes les options pratiques pour que le contenu soit adressé à sa source, ou tout autre moyen alternatif au blocage. Le blocage de contenu ne doit pas être entrepris juste par facilité.

b. **Soyez transparent :** il doit y avoir de la transparence quant au blocage ainsi qu'aux raisons qui motivent son existence. Les autorités nationales doivent veiller à ce que les utilisateurs concernés aient la possibilité de faire part de leurs préoccupations concernant les effets négatifs de ces mesures sur leurs droits et leurs intérêts.

c. **Réfléchissez à votre responsabilité envers l'Internet :** l'entité qui ordonne ou effectue le blocage doit savoir qu'il partage une responsabilité envers le système dans son ensemble pour ne pas nuire à la stabilité, à la sécurité et à la résilience de l'Internet. Les techniques de blocage ont un impact négatif sur la façon dont l'Internet est géré collectivement et fonctionne. Parfois, le dommage est direct, et parfois, il est indirect. Par exemple, les utilisateurs qui contournent le blocage peuvent causer des problèmes ou mettre en péril leur sécurité personnelle.

e. **Pensez globalement, agissez localement :** le blocage et le filtrage locaux peuvent avoir des effets globaux. Mais en général, bloquer le contenu aussi localement que possible minimisera l'impact global. Idéalement, le blocage au point final de l'utilisateur est le plus efficace et minimise les dommages collatéraux.

f. **Impliquez les parties prenantes :** l'élaboration et la mise en œuvre des politiques doivent impliquer un large éventail de parties prenantes, y compris des spécialistes dans les implications technologiques, économiques et de droit des consommateurs, afin de s'assurer que les mesures appropriées sont prises pour minimiser les effets secondaires de telles mesures.

g. **Pensez aux mesures temporaires :** toute mesure de blocage devrait être temporaire. Elle devrait être supprimée dès que la raison du blocage cesse d'exister. Il est assez courant que les contenus illégaux soient déplacés pour échapper aux mesures de blocage, et pourtant les mesures restent souvent en vigueur longtemps après le déplacement du contenu.

h. **Suivez les procédures légales :** tout ordre de blocage de contenu illégal doit être justifié une loi, examiné de manière indépendante et ciblé de manière concrète pour atteindre un but légitime. Les moyens les moins restrictifs disponibles pour adresser les activités illégales doivent être priorisés. Les fournisseurs de services Internet ou d'autres intermédiaires Internet ne doivent pas devenir de facto des agents d'application de la loi: ils ne doivent pas être tenus de déterminer quand la conduite ou le contenu est illégal.

11 Par exemple, des partenariats avec le secteur financier peuvent aider à identifier et limiter les transactions illégales.

Glossaire

CDN Un réseau de diffusion de contenu ou un réseau de distribution de contenu (CDN) est un réseau de serveurs proxy déployés globalement dans plusieurs centres de données. L'objectif d'un CDN est de fournir du contenu aux utilisateurs finaux à haute disponibilité et à haute performance. Les CDN fournissent aujourd'hui une grande partie du contenu sur Internet, y compris les objets Web (texte, graphiques et scripts), les objets téléchargeables (fichiers multimédias, logiciels, documents), les applications (e-commerce, portails), les médias en direct, les médias en diffusion à la demande, et les réseaux sociaux. (https://fr.wikipedia.org/wiki/Content_delivery_network)

Contenu Dans le contexte de cet article, nous utilisons le mot « contenu » en général pour décrire les informations trouvées sur Internet. Ce contenu peut être un document complet ou simplement un paragraphe de texte, une image, une vidéo ou même juste un fichier audio (comme un podcast). Le contenu peut se trouver sur des pages Web vues dans un navigateur, ou il peut être accessible via des outils plus spécialisés tels qu'une application personnalisée.

DNS Le système de noms de domaine (DNS, Domain Name System) est un système hiérarchique de dénomination décentralisée pour les ordinateurs, les services ou d'autres ressources connectés à Internet ou à un réseau privé. Il associe diverses informations aux noms de domaine attribués à chacune des entités participantes. Notamment, il traduit des noms de domaine plus facilement mémorisables en adresses IP numériques nécessaires pour localiser et identifier les services informatiques et les périphériques avec les protocoles réseau sous-jacents. En fournissant un service d'annuaire distribué dans le monde entier, le système de noms de domaine est un élément essentiel de la fonctionnalité d'Internet, utilisé depuis 1985. (https://fr.wikipedia.org/wiki/Domain_Name_System)

DPI L'inspection en profondeur des paquets (DPI, Deep Packet Inspection) est une forme de filtrage de paquets de réseau informatique qui examine la partie de données (et éventuellement aussi l'en-tête) d'un paquet passant par un point d'inspection, en recherchant la non-conformité au protocole, les virus, spam, intrusions ou critères définis pour décider si le paquet peut passer ou s'il doit être traité d'une autre manière, y compris être rejeté. (https://en.wikipedia.org/wiki/Deep_packet_inspection)

Illégal Dans le contexte de cet article, nous utilisons le mot « illégal » pour décrire le contenu interdit dans un contexte national, quelle que soit la raison. Cela peut être un contenu qui est illégal car il s'agit d'une violation du droit d'auteur (ou d'un autre type de propriété intellectuelle), comme un film piraté. Il peut s'agir d'un contenu qui est illégal car il est répréhensible pour des raisons morales, telles que l'obscénité ou la pornographie juvénile. Il peut s'agir d'un contenu qui est illégal parce que les autorités nationales souhaitent le supprimer ou le trouvent offensant, comme une bande dessinée représentant le président du pays de manière défavorable. Un contenu qui est illégal dans une juridiction peut être totalement légal dans une autre. Un contenu qui est illégal dans un contexte (comme une comédie indécente, lorsqu'elle est regardée par des enfants) peut être totalement légal dans un autre contexte (par exemple, lorsqu'il est regardé par des adultes), même dans la même juridiction.

Adresse IP Une adresse IP (abréviation de l'adresse Internet Protocol) est un identifiant attribué à chaque ordinateur et à d'autres périphériques (p. ex. imprimante, routeur, appareil mobile, etc.) connectés à Internet. Elle est utilisée pour localiser et identifier le nœud dans les communications avec d'autres noeuds sur le réseau.
(https://fr.wikipedia.org/wiki/Adresse_IP)

Faux négatif Un faux négatif se produit lorsque le contenu n'est pas bloqué, mais qu'il aurait dû l'être. Par exemple, si les pharmacies illégales sont bloquées, une toute nouvelle pharmacie illégale pourrait ne pas être bloquée si le serveur n'avait pas encore été ajouté à la liste de blocage. Cela s'appellerait un faux négatif.

Faux positif Un faux positif survient lorsque certains contenus sont bloqués, qui n'étaient pas destinés à être bloqués. Par exemple, si la pornographie est bloquée, les informations sur la cuisson des poitrines de poulet pourraient être bloquées si le blocage a utilisé une recherche par mot-clé mal élaborée. Cela serait considéré comme un faux positif.

TLS/SSL Transport Layer Security (TLS) et son prédécesseur, Secure Sockets Layer (SSL), souvent appelé « SSL », sont des protocoles cryptographiques qui fournissent une sécurité de communication sur un réseau informatique. Plusieurs versions des protocoles utilisent largement les applications telles que la navigation sur le Web, le courrier électronique, la télécopie par Internet, la messagerie instantanée et la voix sur IP (VoIP). Les sites Web utilisent TLS pour sécuriser toutes les communications entre leurs serveurs et les navigateurs Web. Le protocole Transport Layer Security vise principalement à assurer la confidentialité et l'intégrité des données entre deux applications informatiques communicantes.
(https://fr.wikipedia.org/wiki/Transport_Layer_Security)

URL Uniform Resource Locator (URL), communément désigné comme une adresse Web, est une référence à une ressource Web qui spécifie son emplacement dans le réseau et un mécanisme pour la récupérer. Les URL sont généralement créées pour référencer les pages Web (https), mais sont également utilisées pour le transfert de fichiers (ftp), le courrier électronique (mailto), l'accès à la base de données (JDBC) et bien d'autres applications. La plupart des navigateurs Web affichent l'URL d'une page Web au-dessus de la page dans une barre d'adresse. Un URL typique peut être https://www.exemple.com/index.html, qui indique un protocole (https), un nom d'hôte (www.exemple.com) et un nom de fichier (index.html).
(https://fr.wikipedia.org/wiki/Uniform_Resource_Locator)

VPN Un réseau privé virtuel (VPN, Virtual Private Network) étend un réseau privé sur un réseau public tel que l'Internet. Il permet aux utilisateurs d'envoyer et de recevoir des données sur des réseaux partagés ou publics comme si leurs appareils informatiques étaient directement connectés au réseau privé. Les applications exécutées sur le VPN peuvent donc bénéficier de la fonctionnalité, de la sécurité et de la gestion du réseau privé.
(https://fr.wikipedia.org/wiki/Réseau_privé_virtuel)

Pour plus d'informations

Les publications suivantes peuvent intéresser les lecteurs à la recherche d'informations complémentaires sur ce sujet (ressources en anglais).

Documents techniques de l'Internet Engineering Task Force

« Enquête sur les techniques de censure dans le monde entier » (projet IETF draft-hall-censorship-tech-04) https://tools.ietf.org/html/draft-hall-censorship-tech-04

« Considérations techniques pour le blocage et le filtrage sur Internet » (RFC 7754) https://tools.ietf.org/html/rfc7754

Politiques publiques, enquêtes et documents de fond

« Filtrage, blocage et suppression de contenu illégal sur Internet », Conseil de l'Europe, 2015. http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

« Liberté d'expression non filtrée : comment le blocage et le filtrage affectent la liberté d'expression » Article 19, 2016. https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

« Liberté sur Internet 2016 », Freedom House, novembre 2016. https://freedomhouse.org/report/freedom-net/freedom-net-2016

« Points de vue de l'Internet Society sur le filtrage du système de noms de domaine (DNS) », Internet Society, 2012. https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf

« Neutralité du réseau », Internet Society, 2015. http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030.pdf

« Points de vue sur les réponses politiques à la violation du droit d'auteur en ligne » Internet Society, 2011. https://www.internetsociety.org/sites/default/files/bp-copyrightpolicy-20110220-en-1.pdf

Remerciements

L'Internet Society remercie chaleureusement Joel Snyder d'Opus One pour sa contribution à ce rapport.

Le rapport a été supervisé par Nicolas Seidler et Andrei Robachevsky de l'Internet Society.

L'article a bénéficié des retours, des commentaires et du soutien de membres du personnel de l'Internet Society : Constance Bommelaer, Sally Wentworth, Olaf Kolkman, Carl Gahnberg, Christine Runnegar, Konstantinos Komaitis, Lia Kiessling, Joyce Dogniez, Kevin Craemer, Bastiaan Quast, Kevin Chege, Dan York, Raquel Gatto.

Un grand merci à l'équipe de communications de l'Internet Society pour l'aspect visuel de ce rapport et la promotion de sa publication : James Wood, Beth Gombala, Lia Kiessling, Allesandra Desantillana.

Enfin, le rapport a été considérablement amélioré grâce à la contribution de plusieurs membres des chapitres locaux de l'Internet Society, membres de l'organisation, membres individuels, ainsi que grâce à la participation du conseil d'administration de l'Internet Society.

Internet Society

internetsociety.org

Galerie Jean-Malbuisson 15,
CH-1204 Genève, Suisse
Tél. +41 22 807 1444

1775 Wiehle Avenue, Suite 201
Reston, Virginia 20190, États-Unis
Tél. +1 703 439 2120