Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet: Visión general

Marzo de 2017

Internet Society

Índice

Prólogo

El uso del bloqueo de Internet por parte de los gobiernos para impedir el acceso a contenido ilegal es una tendencia mundial en ascenso. Existen muchas razones por las cuales los encargados de formular políticas deciden bloquear el acceso a determinado contenido. Algunas de ellas son: juegos y apuestas en línea, propiedad intelectual, protección de los menores y seguridad nacional. Sin embargo, a excepción de los asuntos relacionados con la pornografía infantil, existe poco consenso internacional con respecto a lo que constituye contenido apropiado desde la perspectiva de las políticas públicas.

El objetivo de este artículo es proporcionar una evaluación técnica de los diferentes métodos de bloqueo del contenido de Internet, con información sobre la eficacia de cada método, así como sobre las falencias y los problemas asociados a cada uno de ellos. No pretendemos evaluar la legalidad o las motivaciones políticas del bloqueo del contenido de Internet.[1]

Nuestra conclusión, basada en análisis técnicos, es que el uso del bloqueo de Internet como respuesta a contenido o a actividades ilegales suele ser ineficiente, a menudo no es eficaz y, en general, perjudica involuntariamente a los usuarios de Internet.

Desde el punto de vista técnico, recomendamos a los encargados de formular políticas pensar dos veces antes de considerar el uso de herramientas de bloqueo de Internet para resolver asuntos de políticas públicas. Si lo hacen y deciden utilizar métodos alternativos, será un logro importante en el camino hacia una Internet global, abierta, confiable e interoperable.

1 Los lectores interesados en las evaluaciones legales del bloqueo de contenido pueden consultar los siguientes recursos:
- Artículo 19: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf
- Consejo de Europa: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

Introducción

La transformación de Internet en un fenómeno social mundial le debe mucho al contenido

y a los servicios que se han beneficiado de la arquitectura única de la red. Economías enteras dependen del flujo internacional de contenido. Día a día, las innovaciones pueden alterar industrias completas. Internet ahora es una parte fundamental de los procesos democráticos y los debates políticos. Hay relaciones personales que nacen y terminan en línea.

La tendencia no pierde velocidad. Según los cálculos[2], el tráfico internacional de Internet en 2020 equivaldrá a 95 veces el volumen que tenía toda Internet en 2005. La cantidad de dispositivos conectados a redes IP será tres veces superior a la población mundial en 2020.

Sin embargo, en Internet también hay contenido que los encargados de formular políticas, los legisladores y los organismos de reglamentación de todo el mundo desean bloquear. Desde el bloqueo de sitios extranjeros de apuestas en Europa y América del Norte hasta el bloqueo de discursos políticos en China, el uso de técnicas para evitar el acceso a contenido que se considera ilegal según determinadas leyes nacionales es un fenómeno mundial. La política pública de bloquear contenido en Internet puede obedecer a diversos motivos, que abarcan desde la infracción de las leyes de propiedad intelectual, el material de abuso infantil y las actividades ilegales en línea, hasta la protección de la seguridad nacional.

El objetivo de este trabajo no es evaluar esas motivaciones ni calificar si determinado tipo de bloqueo es bueno o malo desde una perspectiva ética, legal, económica, política o social. Por el contrario, proporcionaremos una evaluación técnica de las ventajas y desventajas de las técnicas de bloqueo que se utilizan con más frecuencia para impedir el acceso al contenido considerado ilegal. El objetivo es ayudar a los lectores a comprender lo que se puede bloquear o no con cada técnica, así como los efectos secundarios, las falencias, los compromisos y los costos asociados.

Nuestra conclusión es que, en general, el uso del bloqueo de Internet para abordar el contenido ilegal es poco eficiente y tiende a ocasionar daños colaterales no intencionales a los usuarios, tal como se resume en la tabla de la página 6.

Desde un punto de vista técnico, **exhortamos a los encargados de formular políticas a pensar dos veces** antes de utilizar estas medidas y los invitamos a priorizar sus respuestas centrándose principalmente en medidas alternativas que ataquen el problema en su origen (vea recomendaciones más detalladas, incluida una guía para reducir al mínimo los efectos negativos de las medidas, al final de este trabajo).

También es importante señalar que este artículo no se centra en las medidas de bloqueo implementadas para la administración regular de redes o por cuestiones de seguridad (p. ej., para responder al spam, o correo electrónico no deseado, o al malware). En esos casos, algunas de las herramientas descritas en este trabajo también suelen ser eficaces para lograr los objetivos deseados.

Información adicional:
¿Filtrado, bloqueo o censura?

Cuando se describe el filtrado en Internet, surgen términos como “filtrado”, “bloqueo”, “cierre” y “censura”, entre muchos otros. Desde el punto de vista del usuario, el término elegido es menos importante que el efecto: la imposibilidad de obtener acceso a una parte de Internet. Para los encargados de formular políticas y los activistas digitales, la elección de un término en particular generalmente obedece más a los matices semánticos que a la corrección técnica. La palabra “censura” tiene una fuerte connotación negativa, mientras que “filtrado” parece denotar una operación más simpática e inocua, como la de quitar las semillas de un vaso de jugo de naranja. En este artículo, hemos optado por usar “bloqueo” como un término simple y directo.

2 Pronóstico VNI (Visual Networking Index) de Cisco®: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking- index-vni/complete-white-paper-c11-481360.html

La siguiente tabla resume los principales inconvenientes asociados con el bloqueo de contenido en Internet por razones de política pública:

Problema	Detalles
Se puede eludir fácilmente	Un usuario suficientemente motivado puede eludir fácilmente todas las técnicas descritas en este artículo. A medida que los usuarios descubren las diversas maneras de burlar el bloqueo de contenido, la eficacia del bloqueo disminuye.
No resuelve el problema	El bloqueo de contenido no elimina el contenido que se considera ilegal. En algunos casos, una prohibición nacional puede ser incompatible con las normas internacionales; sin embargo, cuando existe un amplio acuerdo respecto a la ilegalidad del contenido, la mejor solución es eliminar tal contenido en el origen.
Causa daños colaterales	Cuando el contenido legal e ilegal comparte la misma dirección IP, nombre de dominio u otra característica, el bloqueo impedirá el acceso a todo el contenido, sea legal o ilegal. Por ejemplo, si se utiliza filtrado de DNS para bloquear el acceso a un artículo de Wikipedia, también se bloquearán millones de artículos de Wikipedia.
Pone a los usuarios en riesgo	Cuando el servicio de Internet local no se considera confiable y abierto, los usuarios pueden recurrir a métodos alternativos atípicos, como descargar software para redireccionar el tráfico a fin de evitar los filtros. Estas soluciones precarias someten a los usuarios a riesgos de seguridad adicionales.
Alienta la falta de transparencia	Un entorno confiable y transparente es importante para el buen funcionamiento de Internet. El bloqueo de contenido elimina la transparencia, socava la naturaleza abierta de la red y genera desconfianza en las fuentes de información pública.
Impulsa la clandestinidad de los servicios	Al generalizarse el bloqueo de contenido, se establecerán estructuras superpuestas de redes alternativas y servicios "clandestinos", que impedirán la fácil visualización del contenido por parte de las entidades encargadas de la aplicación de la ley. Por ejemplo, el contenido puede pasar a la Web Oscura o "Dark Web", o los usuarios pueden canalizar el tráfico a través de redes privadas virtuales (VPN).
No respecta la privacidad	Varios tipos de bloqueo de contenido requieren examinar el tráfico del usuario, incluido el tráfico cifrado. Cuando hay terceros que supervisan las actividades de los usuarios de Internet, registran transacciones o quebrantan la seguridad de cifrado básica de Internet, se viola la privacidad de los usuarios.
Genera preocupaciones asociadas a los derechos humanos y al procedimiento debido	Cuando se implementa sin considerar debidamente nociones como la necesidad y la proporcionalidad, el bloqueo de contenido puede ocasionar daños colaterales importantes, restringir las comunicaciones libres y abiertas, e imponer límites a los derechos de los individuos.

Motivaciones para bloquear contenido

En este trabajo, nos centraremos **en el bloqueo debido a políticas públicas** y en sus efectos sobre Internet y los usuarios (consulte el recuadro de "Información adicional" para conocer otras motivaciones del bloqueo de contenido).

Las autoridades nacionales utilizan el bloqueo por políticas públicas para restringir el acceso a información (o a servicios relacionados) que es ilegal en una jurisdicción determinada, que se considera una amenaza para el orden público o que es objetable para una audiencia en particular.

Por ejemplo, la mayoría de los países comparten el deseo de bloquear el acceso de los menores al material obsceno o el acceso de cualquier persona a material de abuso infantil. Según el entorno jurídico local, también se puede bloquear el contenido si infringe las leyes de propiedad intelectual, si se considera una amenaza a la seguridad nacional o si está prohibido por razones culturales o políticas.

Uno de los desafíos que llevan a las autoridades nacionales a aplicar medidas de bloqueo del contenido en Internet es que los actores que entregan el contenido a los consumidores pueden encontrarse en diferentes países, con diferentes leyes que determinan qué es "contenido ilegal" y qué no lo es. Además, debido al entorno global de Internet, detener la fuente de contenido ilegal es más complicado que simplemente apagar un servidor local. Por ejemplo, la persona que proporciona el contenido, los servidores que lo hospedan y el nombre de dominio que apunta al contenido pueden estar en tres países diferentes, y estos tres países pueden escapar a la jurisdicción de una autoridad nacional determinada. Esto pone de relieve la importancia de la cooperación entre jurisdicciones y la necesidad de una estrecha coordinación con los actores no gubernamentales.

Otros tipos de motivaciones para bloquear contenido

En este artículo, nos centramos en el bloqueo por razones de política pública, pero también hay otras dos razones comunes por las que se realizan bloqueos en la red. La primera es **evitar o responder a las amenazas a la seguridad de la red.** Este tipo de bloqueo es muy habitual. Por ejemplo, la mayoría de las empresas intentan bloquear el ingreso de malware a sus redes. Muchos proveedores de servicios de Internet (ISP) bloquean el tráfico malicioso que sale de sus redes, por ejemplo, de dispositivos de IoT secuestrados (como cámaras web). El filtrado del correo electrónico es muy común. Incluye el bloqueo de mensajes masivos no deseados, así como también de mensajes maliciosos, como los de suplantación de identidad (phishing). Este artículo no aborda estos tipos de bloqueo.

La segunda razón por la que se suele bloquear contenido es la **administración del uso de las redes.** Un creciente ámbito de bloqueo de contenido en Internet obedece a requisitos de administración del tiempo, las redes o el ancho de banda, más que a los tipos de contenido. Por ejemplo, es posible que los empleadores deseen restringir el acceso de sus empleados a los sitios de redes sociales sin dejar de ofrecerles acceso a Internet en el escritorio. Los proveedores de servicios de Internet pueden permitir, limitar o acelerar determinado contenido en función de los servicios contratados. La administración del uso de la red rara vez es un asunto de políticas públicas, excepto en los casos de comportamiento monopólico. Los lectores interesados en la neutralidad de la red encontrarán referencias en Lecturas adicionales, en la página 26.

Descripción general de las técnicas de bloqueo de contenido

Cada método tiene limitaciones y consecuencias técnicas y políticas que se deben tener en cuenta al proponer algún tipo de bloqueo de contenido. El objetivo de este artículo es proporcionar un método común para evaluar su eficacia y sus efectos secundarios. Los lectores interesados en un análisis más técnico del bloqueo de contenido encontrarán referencias a los documentos técnicos del IETF en Lecturas adicionales, en la página 26.

Este trabajo evaluará los siguientes tipos de bloqueo de contenido:

- Bloqueo basado en el protocolo y en la IP
- Bloqueo basado en la inspección profunda de paquetes (DPI)
- Bloqueo basado en las URL
- Bloqueo basado en la plataforma (especialmente, en los motores de búsqueda)
- Bloqueo basado en DNS

Elegimos estos cinco tipos de bloqueo porque apuntan a los elementos que intervienen en el ciclo habitual de búsqueda y recuperación de información por parte de los usuarios finales, entre ellos, el uso de motores de búsqueda y la visualización de información con navegadores web o herramientas similares. Los encargados de formular políticas, que también son usuarios de Internet, están muy familiarizados con este ciclo, que abarca las operaciones que la mayoría de los bloqueos debido a políticas públicas intenta interrumpir.

En el diagrama de la derecha, mostramos los pasos que podría seguir un usuario de Internet típico para encontrar información, así como las clases de bloqueo utilizadas para interrumpir el ciclo cuando se implementan bloqueos debido a políticas públicas. En el diagrama, un usuario de Internet busca contenido mediante un motor de búsqueda (paso 1), un punto de partida habitual. El motor de búsqueda devuelve un grupo de resultados (paso 2). El usuario selecciona un resultado y hace clic en él (paso 3). Un tipo de bloqueo, el bloqueo basado en la plataforma, se utiliza para interrumpir esta parte del ciclo impidiendo que el motor de búsqueda devuelva algunos resultados.

El equipo del usuario intenta encontrar el servidor que hospeda los datos en el DNS de Internet (pasos 4 y 5). Un segundo tipo de bloqueo, el bloqueo basado en DNS, se utiliza para interrumpir esta parte del ciclo.

Entonces, el navegador web del usuario intenta conectarse al servidor (paso 6). Esta parte del ciclo se puede bloquear mediante otros tres métodos: bloqueo basado en el protocolo y en la IP, el bloqueo basado en las URL y el bloqueo basado en la inspección profunda de paquetes.

Visión general: pasos del proceso de recuperación y bloqueo de la información en línea

1. El usuario busca "bomba" con un motor de búsqueda.
2. Sin filtrado, el usuario ve un resultado.
3. El usuario hace clic en un resultado (http:/ ejemplo.com/ bomba)
4. La computadora del usuario busca "ejemplo.com" en el DNS para conectar con el servidor web.
5. ejemplo.com = 192.0.222
6. El navegador web del usuario se conecta con el servidor web "ejemplo.com" y solicita la página web específica en la que hizo clic el usuario.
7. De: 192.0.222 Solicitud del servidor ejemplo.com al usuario. Buscar:

ejemplo.com? RESOLUCIÓN DE DNS

PARA: 192.0.222 Solicitud de la PC del usuario al servidor ejemplo.com. Buscar: http:// ejemplo.com/bomba

Si existe un bloqueo, el usuario probablemente vea lo siguiente:

Con el **filtrado de búsquedas** y otros bloqueos basados en plataformas, si el usuario emplea un motor en particular, los resultados quedan fuera de su alcance.	Con el **bloqueo basado en DNS,** la computadora del usuario no encuentra el servidor, de manera que no puede ver la página web. El usuario verá el mensaje "No se encontró el servidor".	Con el **bloqueo basado en la IP y en el protocolo,** se bloquea la conexión con el servidor con IP=192.0.222. El contenido del servidor no está disponible, aunque esta no sea la intención.	Con el **bloqueo basado en URL,** el tráfico se bloquea si la URL está en la lista de direcciones bloquedas.	Con el **bloqueo basado en la inspección profunda de paquetes** (DPI, del inglés Deep Packet Inspection), ciertas palabras clave de la página web pueden activar una interrupción en el tráfico. Existe un riesgo elevado de que se bloquee contenido que no se intentaba bloquear.
No se encontraron resultados para "bomba".	**No se encontró el servidor.**	**Se agotó el tiempo de espera de la conexión.**	**El administrador de red ha bloqueado el sitio.**	**Se restableció la conexión.**

Desde luego, Internet es mucho más que búsquedas y navegadores web, y gran parte de las técnicas analizadas a continuación no son solo eficaces para bloquear páginas web. Por ejemplo, el uso de servicios VPN para cifrar y ocultar tráfico a menudo puede bloquearse utilizando una combinación del bloqueo basado en la inspección profunda de paquetes y el bloqueo basado en el protocolo/la IP.

Estos bloqueos pueden aplicarse de maneras muy específicas (por ejemplo, a un documento concreto en un sitio web determinado) o muy genéricas (por ejemplo, al "material sobre un asunto" o a los "servicios de voz sobre IP").

¿Dónde se da el bloqueo de contenido?

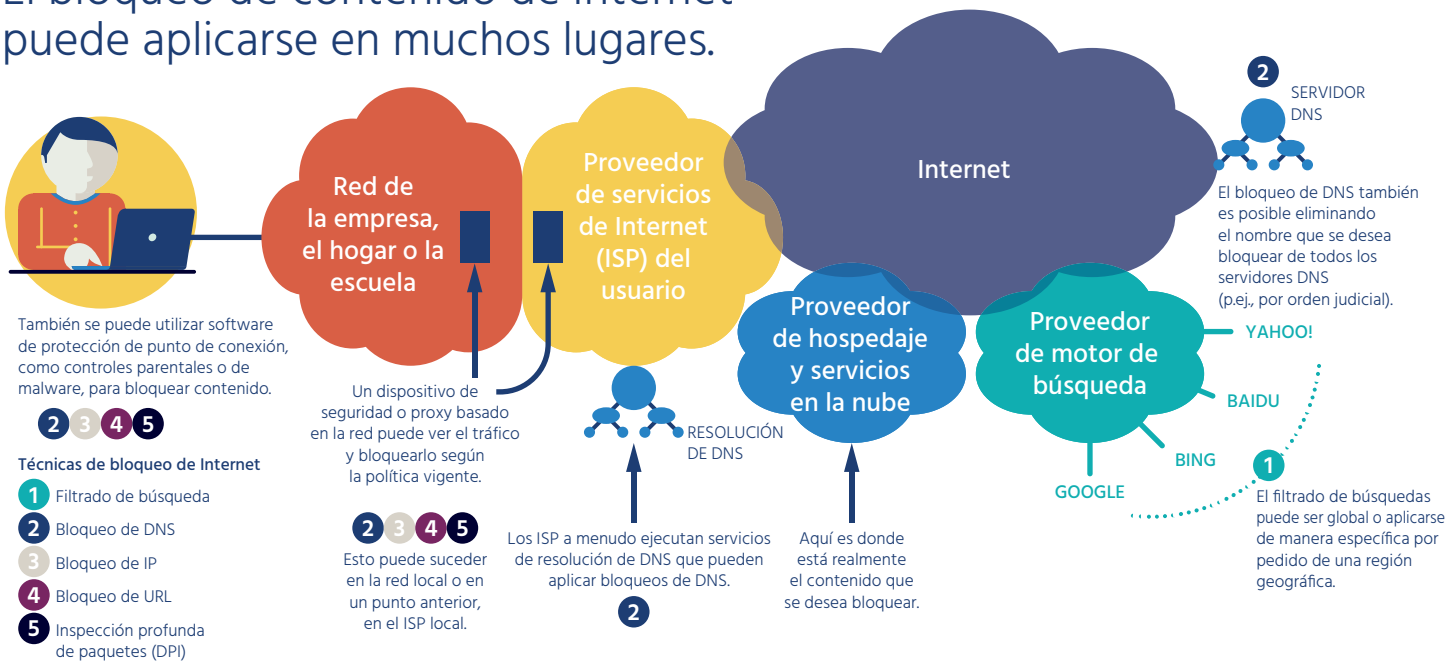
Muchas de las técnicas de bloqueo de contenido analizadas aquí pueden utilizarse en diferentes puntos, como se muestra en la siguiente tabla.

Nivel nacional	Cuando así lo ordena una política gubernamental, todo el tráfico que ingresa o que sale de un país puede estar sujeto a un bloqueo de contenido. Esto requiere un control estricto de todas las conexiones internacionales mediante una puerta de enlace o un firewall nacional, o se puede imponer paralelamente a todos los proveedores e ISP de un país.
Nivel de operador e ISP	Los distintos operadores de telecomunicaciones, incluidos los operadores de servicios móviles y los ISP tradicionales, pueden instalar herramientas de bloqueo.
Nivel de red local	Los dispositivos portátiles y de escritorio de los usuarios finales habitualmente no están conectados directamente a un operador, sino a redes domésticas, corporativas o escolares. Estas redes locales pueden tener bloqueos, por lo general, basados en políticas de seguridad o de administración de redes y no en políticas gubernamentales.
Nivel de punto de conexión	Es posible instalar software que aplique la política de bloqueo directamente en las computadoras de los usuarios finales. Este método se utiliza comúnmente en redes domésticas y corporativas, generalmente por razones de seguridad, pero también para la aplicación de controles parentales o para la administración de redes.

Tenga en cuenta que, cuando el bloqueo obedece a políticas públicas, la mayoría de las medidas se aplican en los dos primeros niveles (nivel nacional y nivel de operador e ISP).

El siguiente diagrama sintetiza algunos de los principales lugares donde puede realizarse el bloqueo y los tipos de bloqueo posibles para cada uno.

El bloqueo de contenido de Internet puede aplicarse en muchos lugares.



Información adicional:
Bloqueo de contenido en el punto de conexión

Este trabajo se centra en el bloqueo de contenido en Internet por políticas públicas.

Sin embargo, es importante observar que uno de los modos más eficaces de bloquear el contenido no deseado es mediante la instalación de software en el dispositivo del usuario, comúnmente denominado "punto de conexión", porque es el último punto de conexión entre el usuario e Internet. La mayoría de los usuarios de computadoras utilizan software en sus dispositivos para bloquear el malware (virus, caballos de Troya y suplantación de identidad), ya sea instalándolo personalmente o a través del grupo de TI de la organización.

Las organizaciones también utilizan software de bloqueo de contenido en los puntos de conexión para bloquear contenido por otras razones. Por ejemplo, las bibliotecas a menudo instalan este tipo de software en las computadoras públicas para bloquear la visualización de pornografía por parte de los visitantes, y los padres pueden utilizarlo para bloquear el acceso de sus hijos a contenido no deseado.

El bloqueo de contenido en el punto de conexión puede utilizar muchas de las técnicas descritas en este trabajo, incluido el análisis de contenido, la categorización de URL, el bloqueo de direcciones IP y la interceptación de DNS. En general, el bloqueo y el análisis se realizan en el punto de conexión propiamente dicho. Sin embargo, los proveedores de este software utilizan cada vez más las herramientas basadas en la nube, incluidas las de exploración de contenido y bloqueo basado en el DNS, en cooperación con una pequeña cantidad de software en los dispositivos o puntos de conexión. En estas soluciones más nuevas, una parte o la totalidad del contenido de Internet puede pasar por un servicio basado en la nube. La ventaja de trasladar la toma de decisiones a la nube es que no es necesario actualizar constantemente los puntos de conexión y que el efecto de la evaluación del contenido sobre el rendimiento pasa de la computadora o el teléfono inteligente del usuario a una nube de computadoras que se escala con facilidad. Sin embargo, el enrutamiento del tráfico a través de un tercero crea problemas de privacidad, porque el contenido queda a disposición del tercero y, si la implementación no es adecuada, surgen problemas de seguridad.

Evaluación de los tipos de bloqueo de contenido

Los cinco tipos de bloqueo de contenido más comunes se diferencian por aquello que bloquean y por el modo en que funcionan.

A continuación, se analizarán con más detalle las técnicas de bloqueo de contenido y se las evaluará según criterios específicos.[3]

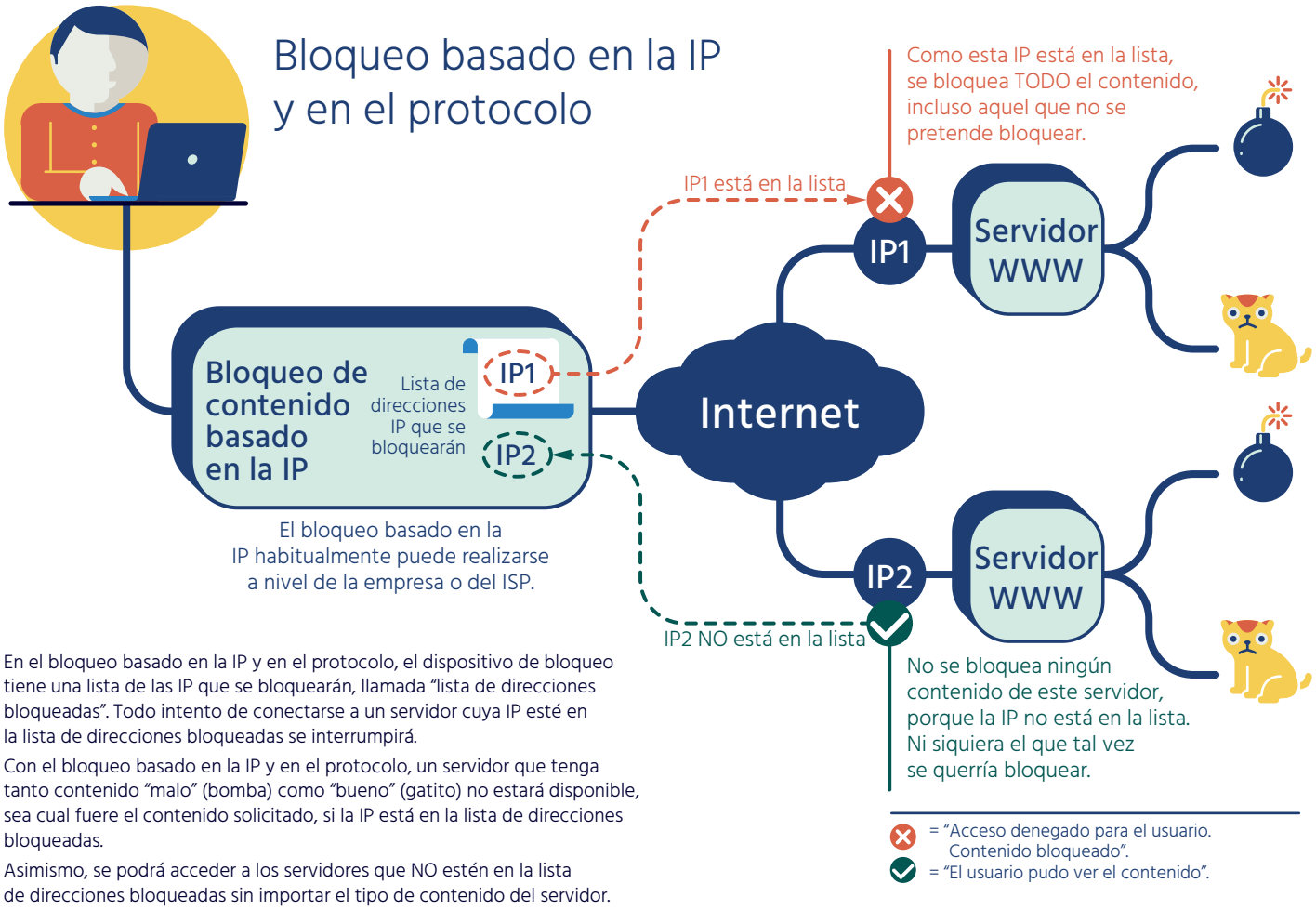
1. **¿Qué usuarios y servicios de Internet se ven afectados por esta técnica?** ¿Qué grupos no están afectados?
2. **¿Cuán específica es la técnica para impedir el acceso a determinado contenido?** ¿Cuánto daño colateral (bloqueos no intencionales) genera esta técnica de bloqueo?
3. **¿Cuán eficaz es esta técnica para bloquear contenido?** ¿Qué tipos de usuarios y proveedores de contenido pueden eludir esta técnica?
4. **¿Cuáles son los efectos secundarios más comunes de esta técnica?** ¿Qué problemas técnicos ocasiona esta técnica? ¿Qué problemas no técnicos (p. ej., efectos sobre la confianza y los derechos fundamentales) surgen de la utilización de esta técnica?

3 Estos criterios se han tomado de la RFC 7754, "Consideraciones técnicas para el bloqueo y el filtrado de servicios de Internet".

Bloqueo basado en el protocolo y en la IP

El bloqueo basado en la IP coloca barreras en la red, como firewalls, que bloquean todo el tráfico hacia un grupo de direcciones IP. El bloqueo basado en el protocolo utiliza otros identificadores de red de bajo nivel, como el número de puerto TCP/IP, que pueden identificar una aplicación específica en un servidor o un tipo de protocolo de aplicación. Estos métodos simples de bloqueo de contenido en realidad no bloquean directamente el contenido, bloquean el tráfico a direcciones IP o a protocolos o puertos TCP/IP conocidos que están asociados a determinado contenido o aplicación. El bloqueo basado en la IP y en el protocolo también puede realizarse instalando software en las computadoras de los usuarios, típicamente, por razones de seguridad de la red.

Por ejemplo, si el objetivo fuera bloquear todo el contenido hospedado en el país mítico de Elbonia, podría utilizarse el bloqueo de IP si se conociera el grupo de direcciones IP que hospedan contenido en Elbonia. Del mismo modo, si el objetivo fuera bloquear todos los servicios VPN (que permiten cifrar el tráfico y ocultar tanto el destino como el contenido), podría utilizarse el bloqueo basado en el protocolo para impedir que los servicios VPN utilicen protocolos o números de puerto TCP/IP conocidos.



En el bloqueo basado en la IP y en el protocolo, el dispositivo de bloqueo tiene una lista de las IP que se bloquearán, llamada "lista de direcciones bloqueadas". Todo intento de conectarse a un servidor cuya IP esté en la lista de direcciones bloqueadas se interrumpirá.

Con el bloqueo basado en la IP y en el protocolo, un servidor que tenga tanto contenido "malo" (bomba) como "bueno" (gatito) no estará disponible, sea cual fuere el contenido solicitado, si la IP está en la lista de direcciones bloqueadas.

Asimismo, se podrá acceder a los servidores que NO estén en la lista de direcciones bloqueadas sin importar el tipo de contenido del servidor.

Una variación del bloqueo de IP consiste en la limitación del tráfico. En este caso, no se bloquea todo el tráfico, sino solo un determinado porcentaje. Los usuarios pueden percibir que el servicio es muy lento o simplemente que funciona con altibajos. Este método puede utilizarse para desalentar a los usuarios de usar un servicio haciéndolo parecer poco confiable, o bien para alentar el uso de servicios alternativos sin revelar que existe un bloqueo. (Esto también puede obedecer a cuestiones relacionadas con la administración de redes y del ancho de banda en una empresa o un ISP).

Tanto el bloqueo basado en la IP como el basado en el protocolo utilizan dispositivos ubicados entre el usuario y el contenido y, por lo tanto, requieren que quien aplica el bloqueo (por ejemplo, el ISP del usuario) tenga control absoluto sobre la conexión entre el usuario e Internet. Un usuario que no se encuentre "detrás" del dispositivo de bloqueo o que utilice tecnología como una VPN, que oculta el verdadero destino del tráfico, no se verá afectado por este tipo de bloqueo.

Por lo general, el bloqueo de IP es una técnica de filtrado poco eficaz, difícil de mantener correctamente y con un alto nivel de bloqueos adicionales no intencionales, y que puede ser eludido fácilmente por editores que transfieren el contenido a nuevos servidores (con nuevas direcciones IP).

El bloqueo de IP tampoco funciona cuando los proveedores de información utilizan redes de entrega de contenido (CDN), ya que las direcciones IP de la información son sumamente dinámicas y cambian constantemente.[4] Las CDN también utilizan la misma dirección IP para varios clientes y tipos de contenido diferentes, lo que genera un alto nivel de interrupciones involuntarias en el servicio.

El bloqueo de la IP y el protocolo funcionan mejor cuando se utilizan para bloquear aplicaciones específicas más que contenido específico. Por ejemplo, el tráfico VPN se puede interrumpir mediante bloqueos del protocolo y de los puertos TCP/IP, combinados con bloqueos de las direcciones IP de servicios VPN públicos conocidos. Esta es una técnica común sumamente eficaz.

El bloqueo de IP también es el método más eficaz cuando el contenido está hospedado en un servidor de un centro de datos específico o cuando existe preocupación por un conjunto de archivos muy concreto. El bloqueo basado en la IP no es muy eficaz para servicios de hospedaje de mayores dimensiones, que están distribuidos en muchos centros de datos o que utilizan redes de distribución de contenido (CDN) para agilizar el acceso.

4 Una red de distribución de contenido es una gran red de servidores geográficamente dispersos que agiliza la entrega de contenido web a los usuarios de Internet. Para agilizar el acceso al contenido de los clientes, las grandes CDN tienen cientos de miles de servidores en numerosos países. Estas redes almacenan copias del contenido de texto, imágenes, audio y video de los clientes en servidores propios ubicados en el "perímetro" de Internet. De este modo, las solicitudes de los usuarios pueden ser atendidas por un servidor perimetral cercano en lugar de recurrir a los servidores centralizados del cliente.

Bloqueo basado en la inspección profunda de paquetes (DPI)

El bloqueo basado en la inspección profunda de paquetes usa dispositivos entre el usuario final y el resto de Internet para filtrar por contenido, patrones o tipos de aplicaciones específicos. Este tipo de bloqueo hace un uso intensivo de recursos informáticos y, en consecuencia, es costoso, porque se debe evaluar todo el contenido para determinar si cumple las reglas de bloqueo. El bloqueo basado en DPI también puede realizarse instalando software en las computadoras de los usuarios, típicamente, para la seguridad de la red.

Para ser eficaz, el bloqueo DPI requiere algún tipo de firma o información sobre el contenido. Pueden ser contraseñas, características del tráfico (como el tamaño de los paquetes o las velocidades de transmisión), nombres de archivos u otra información específica del contenido. El bloqueo DPI es muy eficaz para bloquear o limitar determinadas aplicaciones (como el uso compartido de archivos punto a punto o el tráfico de voz sobre IP [VoIP]) y tipos de archivos de datos (como los archivos multimedia).

En el bloqueo basado en DPI, el dispositivo de bloqueo posee una lista de contenido para bloquear, que se identifica mediante palabras clave u otras técnicas (incluido el cotejo de imágenes). Todo intento de descargar contenido no cifrado que coincida con la lista se interrumpirá.

Con la DPI, son habituales los falsos positivos (contenido que se bloquea incorrectamente) y los falsos negativos (contenido que no se bloquea según lo deseado). También es difícil hacer una correcta DPI cuando el tráfico es cifrado.

En este diagrama, la "bomba" se bloquea porque coincide con el contenido. Sin embargo, aunque el operador del dispositivo de DPI quisiera bloquearla, la "dinamita" no sería bloqueada porque no coincide con la lista de contenido bloqueado.

El bloqueo DPI se utiliza muy comúnmente en los sistemas de protección contra la fuga de datos, los productos antispam y antimalware (antivirus) y en la administración de redes con priorización del tráfico (por ejemplo, aumentando la prioridad de las videoconferencias empresariales) de las empresas. Sin embargo, también se puede utilizar para el bloqueo basado en políticas. Por ejemplo, el uso de servicios VoIP que no son proporcionados por un operador nacional de telecomunicaciones a menudo está reglamentado o restringido, y el bloqueo DPI es eficaz para aplicar esas restricciones.

El bloqueo DPI utiliza dispositivos que pueden ver y controlar todo el tráfico entre el usuario final y el contenido. En consecuencia, la parte que aplica el bloqueo (por ejemplo, el ISP del usuario) debe tener control completo sobre la conexión del usuario final a Internet. Cuando el tráfico está cifrado, como sucede a menudo, los sistemas de bloqueo basados en DPI pueden no ser tan eficaces. Esto se analiza en más detalle en el recuadro de información adicional "Desafíos del cifrado, los proxy y el bloqueo", a la derecha.

El bloqueo DPI generalmente es una técnica eficaz para bloquear determinados tipos de contenido que se pueden identificar mediante firmas u otras reglas (por ejemplo, "bloquear todo el tráfico de voz sobre IP"). El bloqueo DPI ha tenido mucho menos éxito con otros tipos de contenido, como ciertos archivos multimedia o documentos que contienen palabras claves específicas. Como el bloqueo DPI examina todo el tráfico hacia los usuarios finales, también invade la privacidad de los usuarios.

La eficacia general del bloqueo DPI depende ampliamente de los objetivos y las herramientas de DPI específicas que se utilicen. Por lo general, las herramientas de DPI son más eficaces para la administración de redes y la aplicación de medidas de seguridad, y no se adaptan bien al bloqueo basado en políticas.

Información adicional:
Desafíos del cifrado, los proxy y el bloqueo

Varias de las técnicas analizadas en este artículo, incluido el bloqueo basado en la inspección profunda de paquetes (DPI) y el bloqueo basado en las URL, tienen una limitación muy real: deben ser capaces de ver el tráfico que se está evaluando. Los dispositivos situados en la red no pueden bloquear de manera fehaciente los servidores web que ofrecen cifrado o los usuarios que cifran sus comunicaciones (por lo general, mediante tecnología de cifrado específica para aplicaciones, como TLS/SSL). Muchas de las otras técnicas mencionadas también pueden eludirse fácilmente cuando el usuario tiene acceso a tecnología la VPN que cifra las comunicaciones y oculta el verdadero destino y tipo de tráfico. Aunque los investigadores y los proveedores han desarrollado formas de identificar ciertos tipos de tráfico mediante inferencia y análisis, estas técnicas a menudo simplemente adivinan el tipo de tráfico que están viendo.

En una investigación reciente, realizada en febrero de 2016, el 49 % del tráfico web en EE. UU. (por volumen) estaba cifrado. (Consulte: http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf) Este tráfico sería efectivamente invisible para el bloqueo basado en URL y las herramientas de DPI que observan el contenido, porque la única información visible sería el nombre de dominio del servidor que hospeda la información. Para compensar esta "invisibilidad", algunos bloqueos de red utilizan dispositivos (llamados proxy) que interceptan y descifran el tráfico entre el usuario y el servidor web, lo que ocasiona una ruptura en el modelo de cifrado de extremo a extremo de TLS/SSL.

Cuando se utilizan proxy, surgen importantes preocupaciones en materia de seguridad y privacidad. Al romper el modelo TLS/SSL, la parte que aplica el bloqueo obtiene acceso a todos los datos cifrados y, de manera no intencional, puede permitir que otros lo hagan. El proxy también podría cambiar el contenido. Si la parte que aplica el bloqueo controla el sistema del usuario (p. ej., un dispositivo con administración corporativa estaría sumamente controlado), el proxy puede ser muy transparente. Sin embargo, la presencia de un proxy en general es evidente para el usuario final, al menos en el tráfico cifrado con TLS/SSL (p. ej., el usuario puede recibir una alerta que indica que el certificado no proviene de una autoridad de confianza). Además, las nuevas normas del IETF y del sector (como la seguridad estricta de transporte HTTP [RFC 6797], la fijación o pinning de claves públicas para HTTP [RFC 7469] y la autenticación basada en DNS de entidades con nombre [RFC 6698]) y las nuevas características de seguridad de los navegadores de Internet modernos hacen más difícil interponer un proxy (y descifrar) el tráfico TLS/SSL sin el conocimiento y la cooperación del usuario final.

Los proxy instalados para el bloqueo de contenido también pueden generar cuellos de botella que afectan el rendimiento del tráfico de la red y hacen que los servicios resulten lentos o poco confiables.

Bloqueo basado en URL

El bloqueo basado en URL es un método muy difundido y puede aplicarse tanto a una computadora en particular como a un dispositivo de red ubicado entre la computadora y el resto de Internet. Este método de bloqueo funciona con aplicaciones web y no se utiliza para bloquear aplicaciones que no están basadas en la web (como VoIP). En el bloqueo de URL, un filtro intercepta el flujo de tráfico web (HTTP) y comprueba si la URL, que aparece en la solicitud HTTP, se encuentra incluida en una base de datos local o en un servicio en línea. Según la respuesta, el filtro de URL permitirá o bloqueará la conexión al servidor web solicitado.

En general, las URL se administran por categoría (como "sitios de deportes"), y se bloquea, se limita o se habilita la categoría completa[5]. Cuando según una política nacional se requiera el bloqueo de URL, lo más probable es que el gobierno administre el servicio en línea y la política de bloqueo. El filtro de URL puede simplemente interrumpir el tráfico o redirigir al usuario a otra página web mostrándole una declaración de política o señalando que el tráfico se ha bloqueado. El bloqueo de URL en la red puede aplicarse mediante proxy y también mediante firewalls y enrutadores.

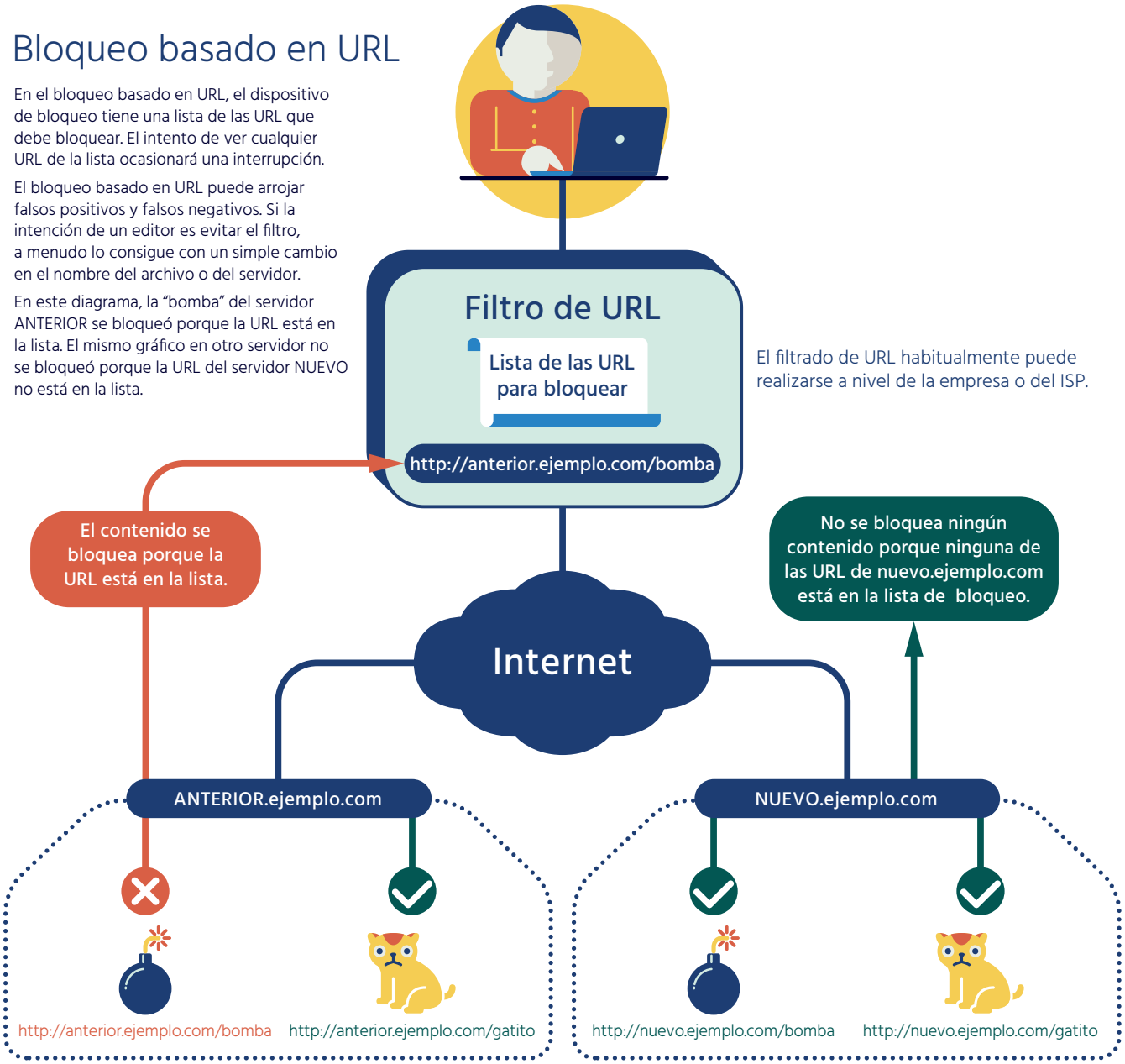
5 Las categorías de filtrado de URL son establecidas por los proveedores de servicios de seguridad y, a menudo, se basan en una combinación del análisis de las páginas web realizado por personas con la exploración automatizada del contenido de dichas páginas. Aunque la mayoría de los proveedores de servicios de seguridad ofrecen bases de datos de filtrado de URL para administrar el tráfico en las redes corporativas, estas bases de datos también se pueden utilizar en otros contextos, como los descritos en este artículo.

Bloqueo basado en URL

En el bloqueo basado en URL, el dispositivo de bloqueo tiene una lista de las URL que debe bloquear. El intento de ver cualquier URL de la lista ocasionará una interrupción.

El bloqueo basado en URL puede arrojar falsos positivos y falsos negativos. Si la intención de un editor es evitar el filtro, a menudo lo consigue con un simple cambio en el nombre del archivo o del servidor.

En este diagrama, la "bomba" del servidor ANTERIOR se bloqueó porque la URL está en la lista. El mismo gráfico en otro servidor no se bloqueó porque la URL del servidor NUEVO no está en la lista.



El bloqueo de URL requiere que quien aplica el bloqueo (por ejemplo, el ISP del usuario) pueda interceptar y controlar el tráfico entre el usuario final e Internet. El bloqueo de URL suele ser costoso, porque el dispositivo de filtrado generalmente debe estar ubicado entre el usuario e Internet y, por lo tanto, requiere un elevado nivel de recursos para que su rendimiento sea aceptable.

Por lo general, el bloqueo de URL se considera muy eficaz para identificar contenido que puede estar en diferentes servidores o servicios, porque la URL no se modifica aunque cambie la dirección IP del servidor. En algunos casos, es posible que el bloqueo de URL no logre impedir completamente el tráfico si las URL son muy complicadas o cambian con frecuencia. Esto puede ser consecuencia de que un editor de información decida, de manera deliberada, eludir activamente el bloqueo por filtrado de URL, o bien puede ser un efecto secundario de algunos sistemas avanzados de publicación, como los que se utilizan para las grandes publicaciones en línea.

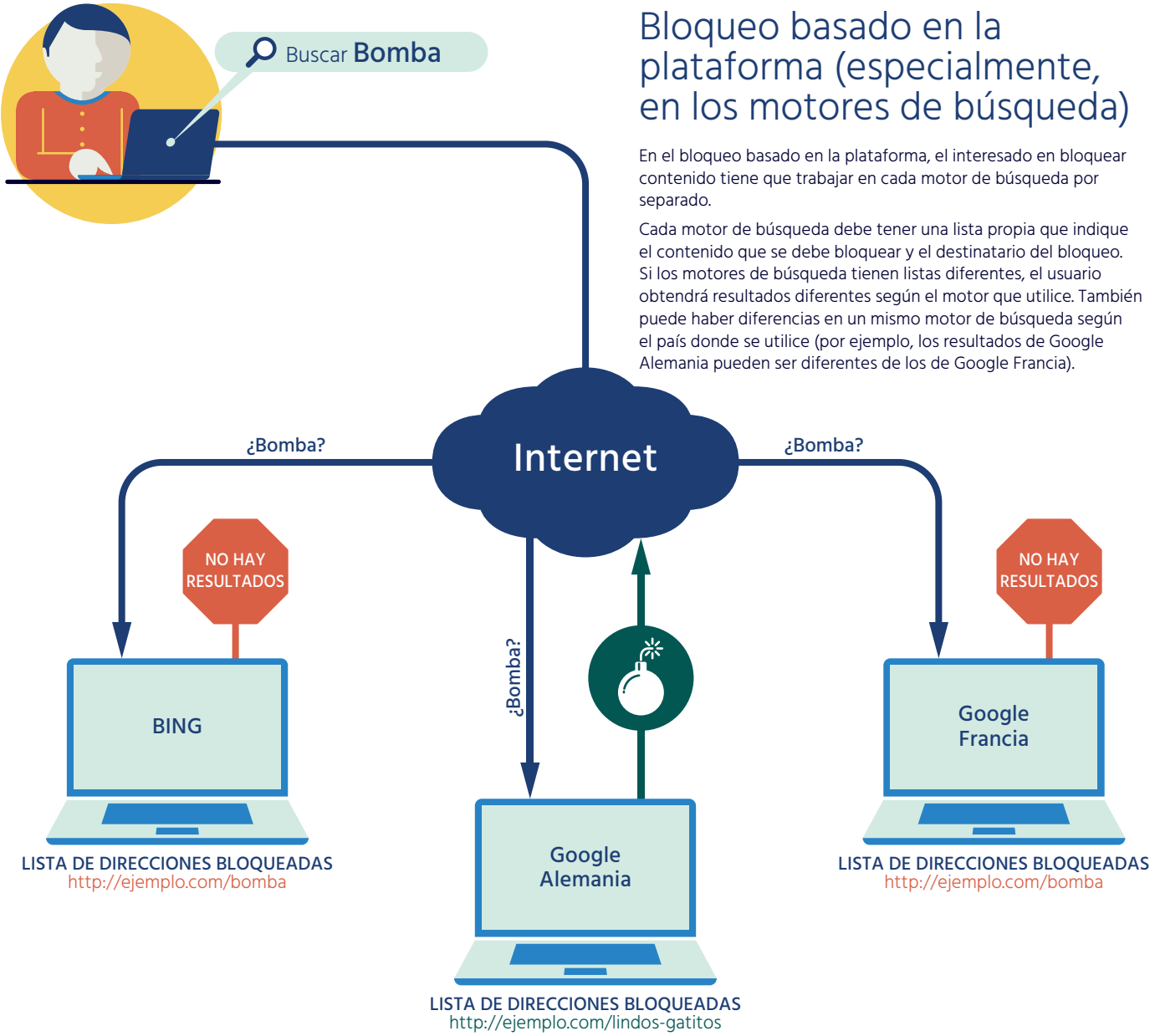
El bloqueo de URL habitualmente es eficaz en las URL de mayor nivel, como una página web determinada, pero pierde eficacia cuando se trata de vínculos profundos (como secciones específicas de contenido dentro de una página web). La eficacia del bloqueo de URL depende del modo en que el usuario ha accedido al contenido: si el usuario tiene un "vínculo profundo" que no está cubierto por el filtro de URL, se permitirá el acceso al contenido. Por ejemplo, el sitio web de Playboy incluye las URL de playboy.com, pero también tiene contenido incrustado que utiliza el nombre de dominio "playboy.tv". Un filtro de URL que no incluyera la URL "playboy.tv" no bloquearía el contenido de video.

Todos los tipos de bloqueo de URL dependen mucho de la calidad del filtro. Un filtro mal diseñado o demasiado amplio puede bloquear tráfico de manera no intencional o tener otros efectos negativos en la experiencia del usuario, como afectar la carga o el formato de las páginas web cuando se bloquea algún componente.

Tal como sucede con los bloqueos por inspección profunda de paquetes, el bloqueo de URL requiere algún tipo de proxy para ver la URL completa cuando el tráfico está cifrado con HTTPS (TLS/SSL). Consulte el recuadro de información adicional "Desafíos del cifrado, los proxy y el bloqueo", en la página 15, para obtener más información acerca de los efectos sobre la privacidad del usuario final. En el tráfico cifrado, el bloqueo de URL solo ve la dirección IP del servidor, no la URL completa, lo que aumenta considerablemente la cantidad de bloqueos no intencionales. Como los proxy son costosos y resultan invasivos para la experiencia del usuario, el bloqueo de URL no funciona bien como herramienta para el bloqueo basado en políticas.

Bloqueo basado en la plataforma (especialmente, en los motores de búsqueda)

E En algunos casos, las autoridades nacionales trabajan con grandes proveedores de servicios informativos para bloquear información en su región geográfica sin bloquear toda la plataforma. Los casos más comunes de filtrado basado en la plataforma se dan en grandes proveedores de motores de búsqueda y en plataformas de medios sociales. Recientemente, también se ha informado que las tiendas de aplicaciones móviles (como Apple Store y Google Play) están trabajando con algunas autoridades nacionales para bloquear la descarga de aplicaciones específicas en sus países.



Bloqueo basado en la plataforma (especialmente, en los motores de búsqueda)

En el bloqueo basado en la plataforma, el interesado en bloquear contenido tiene que trabajar en cada motor de búsqueda por separado.

Cada motor de búsqueda debe tener una lista propia que indique el contenido que se debe bloquear y el destinatario del bloqueo. Si los motores de búsqueda tienen listas diferentes, el usuario obtendrá resultados diferentes según el motor que utilice. También puede haber diferencias en un mismo motor de búsqueda según el país donde se utilice (por ejemplo, los resultados de Google Alemania pueden ser diferentes de los de Google Francia).

El bloqueo basado en la plataforma es una técnica que requiere asistencia del propietario de la plataforma, por ejemplo, el operador de un motor de búsqueda como Google o Microsoft. Con esta técnica, las consultas que determinado grupo de usuarios de Internet envíe a un motor de búsqueda mostrarán un resultado diferente del que obtendrá el resto de Internet, ya que se filtrará todo aquello que apunte a contenido que es, de algún modo, objetable. En algunos casos, la definición de lo que debe bloquearse responde a requisitos gubernamentales y a reglamentaciones locales, pero también puede deberse a preocupaciones del operador del motor de búsqueda. Por ejemplo, un motor de búsqueda puede bloquear los enlaces a malware o a contenido que, según sus propios términos de servicio, es inadecuado.

Como el bloqueo mediante motores de búsqueda requiere la cooperación del proveedor del motor de búsqueda, su uso se limita a dos escenarios muy específicos: la aplicación de reglas a nivel de un país (bloqueo de contenido según reglas específicas para un país o una región) y la aplicación de reglas basadas en la edad (bloqueo de material inadecuado para menores).

El bloqueo mediante motores de búsqueda solo afecta a los usuarios que eligen un motor de búsqueda determinado y solo lo hace cuando se determina que los usuarios cumplen con una serie de reglas de filtrado en particular. En el bloqueo por edad, como SafeSearch[6] (una funcionalidad que ofrecen los principales proveedores de motores de búsqueda y contenido), es necesario dar consentimiento de manera explícita.

Como el bloqueo mediante motores de búsqueda solo filtra los enlaces o "punteros" al contenido y no el contenido propiamente dicho, es una técnica sumamente ineficaz y puede resultar en que, de manera no intencional, atraiga mayor atención al contenido bloqueado. La presencia de numerosos motores de búsqueda, así como el uso de métodos alternativos para encontrar contenido, hacen que este tipo de bloqueo sea muy difícil de aplicar.

Aunque el bloqueo mediante motores de búsqueda parece hacer poco para bloquear contenido, la técnica es muy popular en ámbitos nacionales: se sabe que gobiernos de todo el mundo exigen a los principales motores de búsqueda la implementación de filtros acordes a las normas de sus países, como las destinadas a evitar la infracción de las leyes de copyright o el uso de determinados tipos de discursos que la ley nacional prohíbe. Por ejemplo, en 2015 Google informó que había recibido 8398 solicitudes de 74 tribunales nacionales para eliminar 36 834 resultados de sus búsquedas[7]. Las solicitudes por infracción de las leyes de copyright por parte de individuos también son muy populares: en junio de 2016, Google informó que, durante ese mes, 6937 titulares de derechos de copyright le habían solicitado que eliminara más de 86 millones de resultados de búsqueda[8].

Los individuos también utilizan el bloqueo mediante motores de búsqueda como parte del denominado "derecho al olvido". Bajo este derecho, se ha solicitado el bloqueo de más de un millón de URL a nivel mundial en los últimos dos años (entre mayo de 2014 y junio de 2016).

Información adicional:
Bloqueo en otras plataformas

Aunque el bloqueo mediante motores de búsqueda es el método bloqueo de plataforma más habitual, también suelen considerarse para esta técnica otras plataformas con enormes comunidades de usuarios. Algunos ejemplos comunes son Facebook (que tiene más de 1,5 mil millones de usuarios activos por mes) y YouTube (con más de mil millones de usuarios individuales). Los intentos de utilizar técnicas de bloqueo basado en la URL o en la red para bloquear elementos de contenido individuales, por ejemplo, un artículo periodístico en particular, son muy complicados. Las autoridades nacionales no quieren ser vistas como responsables del bloqueo de plataformas enteras (como Facebook, por ejemplo). En consecuencia, se han propuesto trabajar con los principales proveedores de plataformas para filtrar determinados tipos de contenido que ellas consideran ilegales.

Hay muy poca información acerca de la eficacia, el alcance o los efectos secundarios de otros tipos de bloqueos de plataformas, ya que esta técnica no se ha analizado de manera extensa y fiable en otras plataformas aparte de los motores de búsqueda. Aunque las principales plataformas, como Facebook, YouTube y Twitter, bloquean universalmente determinado tipo de contenido (como el malware o el material pornográfico) y suministran contenido personalizado a sus usuarios, no se dispone de información sobre los bloqueos concretos en ámbitos nacionales.

6 SafeSearch es una funcionalidad disponible en los principales motores de búsqueda, como Google Search, Microsoft Bing y Yahoo!, que bloquea los resultados de búsqueda que contienen "imágenes inadecuadas o explícitas".

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

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

Bloqueo de contenido basado en el DNS

El bloqueo de contenido basado en el DNS es la solución a uno de los problemas que presentan otras técnicas: el impacto sobre el costo y el rendimiento derivado de tener que filtrar todo el tráfico de la red. El bloqueo de contenido basado en el DNS, por el contrario, se centra en el examen y el control de las consultas de DNS.

En este método, la resolución de DNS especializada (consulte Descripción general de DNS en el cuadro de información adicional) cumple dos funciones: además de realizar búsquedas de DNS, comprueba si los nombres aparecen en una lista de direcciones bloqueadas. Cuando la computadora de un usuario intenta utilizar un nombre bloqueado, el servidor especial devuelve información incorrecta, como la dirección IP de un servidor con un aviso que explica que el contenido se ha bloqueado. Otra posibilidad es que el servidor indique que el nombre no existe. El resultado es que el usuario no puede acceder fácilmente al contenido utilizando determinados nombres de dominio.

Como sucede con todos los bloqueos basados en la red, el bloqueo basado en el DNS solo es eficaz cuando la organización que bloquea tiene control absoluto sobre la conexión de red del usuario final. Si el usuario puede seleccionar otra conexión o utilizar otro grupo de servidores de DNS, la técnica no lo afecta. Por ejemplo, cuando Turquía bloqueó algunas consultas de DNS en 2012, los usuarios cambiaron sus sistemas para utilizar los populares servidores de DNS públicos de Google y, de este modo, evitar el bloqueo. Las autoridades turcas respondieron secuestrando todo el tráfico hacia el servicio DNS de Google, lo que ocasionó importantes daños colaterales. El bloqueo de contenido basado en el DNS requiere firewalls u otros dispositivos capaces de interceptar y redireccionar todas las consultas de DNS a los servidores de DNS especializados para el bloqueo. De lo contrario, no será muy eficaz.

La eficacia del bloqueo de contenido basado en el DNS es similar a la del bloqueo basado en la IP. Es un poco más eficaz, porque es más fácil mantener actualizada la lista de nombres de dominio y, además, esta es más exacta que una lista de direcciones IP para la mayoría de los tipos de bloqueo de contenido. Sin embargo, es un poco menos eficaz, porque cambiar nombres de dominio es más sencillo que cambiar direcciones IP, de manera que los editores de información y los usuarios pueden eludir el bloqueo con más facilidad.

Una forma alternativa de bloqueo de contenido basado en el DNS consiste en quitar o eliminar completamente los nombres de dominio del DNS. Este método es más difícil de eludir y el daño colateral es algo limitado. En muchos casos, cuando se recibe una solicitud o una orden judicial de una jurisdicción diferente de aquella en la que opera el registrador o en la que se encuentra el registro, su utilidad depende de la eficacia de la cooperación internacional.

El bloqueo basado en el DNS presenta inconvenientes similares a los del bloqueo basado en la dirección IP: como el contenido prohibido y el permitido pueden coexistir en un mismo servidor con un mismo nombre (como "facebook.com"), se bloquea todo el contenido. Además, la modificación de las respuestas del DNS puede ocasionar otros problemas técnicos que interrumpen otros servicios válidos[9].

La eficacia del bloqueo de contenido basado en el DNS también depende de que el usuario respete las reglas generales de Internet y utilice el servicio DNS estándar para traducir los nombres en direcciones IP. Los usuarios que tienen control absoluto sobre sus computadoras y poseen algunos conocimientos técnicos pueden reconfigurarlas para eludir el servicio DNS estándar y utilizar alternativas, o simplemente pueden almacenar localmente una lista de traducciones de nombres en direcciones.

Información adicional: Descripción general de DNS

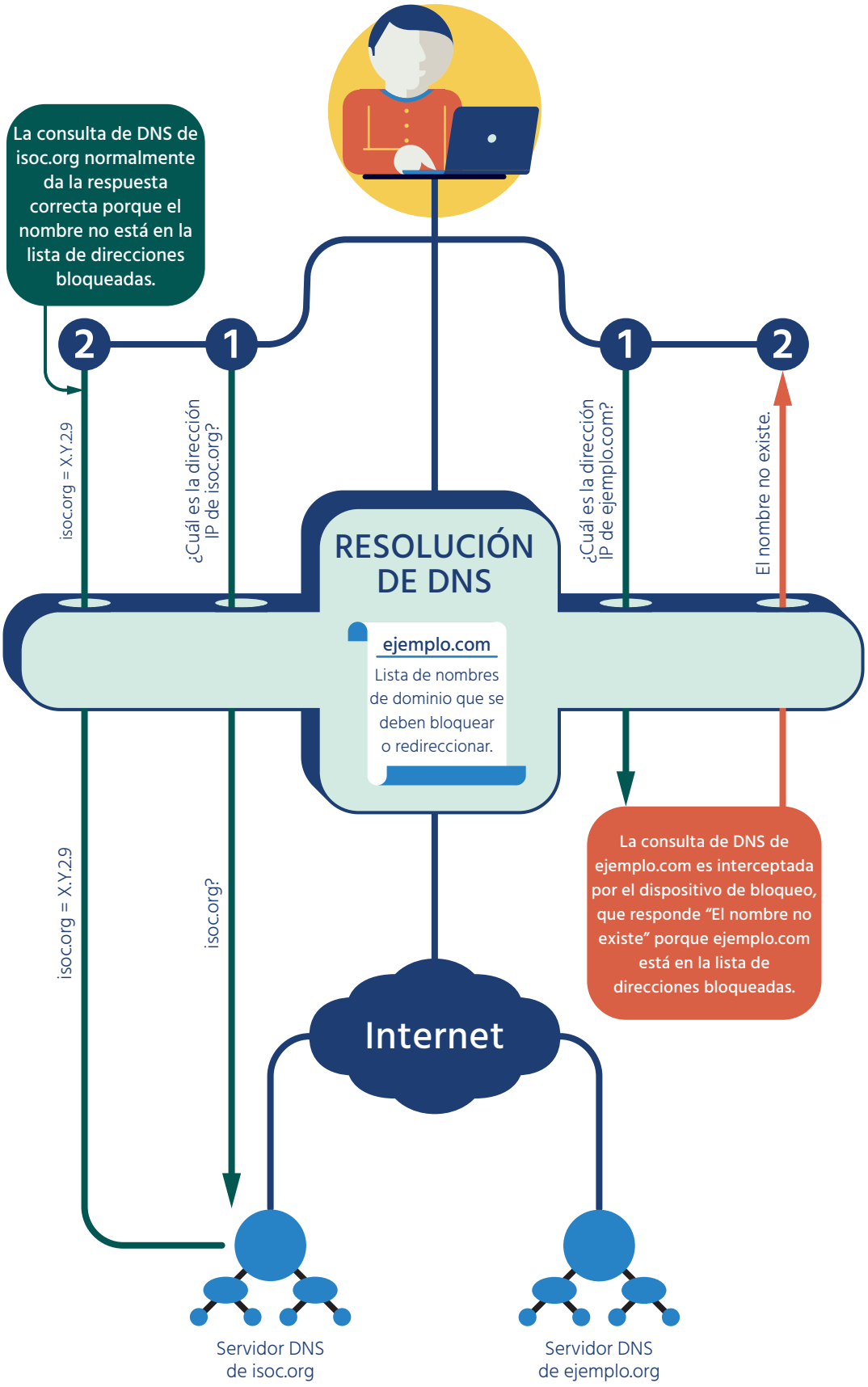
El DNS es un sistema conceptualmente simple que permite buscar una cadena de etiquetas (como "www", "isoc" y "org") separadas por puntos (el nombre de dominio) en una base de datos distribuida en múltiples servidores DNS. La búsqueda de nombres de dominio da una respuesta (por ejemplo, una dirección IP o un sitio web), o bien responde que el nombre no existe.

El tipo de búsqueda de DNS más común es de direcciones IP (protocolo de Internet). Es el tipo de búsqueda que se realiza cada vez que un usuario escribe una URL en un navegador web, por ejemplo. Normalmente, la aplicación (p. ej., el navegador web) no realiza la búsqueda completa, que consta de varios pasos. En lugar de eso, utiliza un sistema intermedio, llamado "de resolución" (porque resuelve las búsquedas de nombres de DNS), que busca en la base de datos distribuida de DNS para recuperar la información solicitada.

Cuando se aplica un bloqueo de contenido basado en DNS, se modifica el funcionamiento normal de la resolución.

9 Los lectores interesados en obtener más detalles pueden consultar el informe "Perspectiva de Internet Society sobre el filtrado de sistemas de nombres de dominios (DNS)" en https://www.internetsociety.org/es/perspectiva-de-internet-society-sobre-el-filtrado-de-sistemas-de-nombres-de-dominios-dns

Bloqueo basado en el DNS



En el bloqueo basado en DNS, el dispositivo de bloqueo tiene una lista de nombres DNS para bloquear.

Como la mayoría de las conexiones de Internet requieren traducir el nombre DNS en una dirección IP, el bloqueo de la consulta y la obtención de una falsa respuesta pueden desalentar a los usuarios de intentar recuperar el contenido bloqueado o de conectarse por otros medios con los servicios bloqueados (p. ej., escribiendo la dirección IP directamente).

Resumen del bloqueo de contenido

Técnicas de bloqueo de contenido en Internet					
	Bloqueo basado en el protocolo y en la IP	**Bloqueo basado en la inspección profunda de paquetes (DPI)**	**Bloqueo basado en URL**	**Bloqueo basado en la plataforma (especialmente, en los motores de búsqueda)**	**Bloqueo basado en el DNS**
Descripción general	Se coloca en la red un dispositivo que aplica un bloqueo por dirección IP o por aplicación (p. ej., VPN).	Se coloca en la red un dispositivo que aplica un bloqueo por palabra clave u otro contenido (p. ej., nombre de archivo).	Se coloca en la red un dispositivo que intercepta las solicitudes web y busca las URL en una lista de direcciones bloqueadas.	En colaboración con los proveedores de aplicaciones (como los motores de búsqueda), se modifica el contenido según los requisitos locales.	A nivel de la red o del ISP, el tráfico de DNS se canaliza a un servidor de DNS modificado que bloquea las búsquedas de ciertos nombres de dominio.
¿Es eficaz?	Como es fácil modificar las direcciones IP y cambiar de lugar el contenido, **esta técnica no funciona bien.** Solo da resultado cuando el editor de la información no busca eludir el bloqueo activamente.	Es muy eficaz cuando la información bloqueada es fácil de caracterizar. Para realizar bloqueos generales (p. ej., "bloquear contenido para adultos") o cuando existe cifrado, **la técnica es muy ineficaz**.	Es una técnica común que **funciona bien para bloquear el acceso a categorías completas** de información. Las páginas nuevas y los sitios pequeños se cuelan fácilmente, al igual que los servidores web cifrados.	Como no hay un monopolio de motores de búsqueda (por ejemplo) y las preferencias de los usuarios cambian constantemente, **este bloqueo es más que nada cosmético y no funciona bien.**	Los editores de contenido y los usuarios finales pueden fácilmente sortear el bloqueo de DNS. Solo es eficaz cuando cada nombre tiene muy poco contenido y debe bloquearse todo ese contenido. **Los desafíos técnicos, el bloqueo excesivo y la fácil evasión hacen que la técnica sea ineficaz.**
¿Quién se ve afectado?	Cualquier persona que esté "detrás" del dispositivo se ve afectada.	Cualquier persona que esté "detrás" del dispositivo se ve afectada.	Los usuarios "detrás" del dispositivo para quienes el dispositivo puede interceptar y evaluar el tráfico web.	Los usuarios del motor de búsqueda que ha instalado el bloqueo.	Los usuarios del servidor DNS. El bloqueo puede aplicarse a nivel de la red o del proveedor de servicios.
¿Qué tan específico es?	**Afecta todo el contenido de un servidor, sea ilegal o no.** Funciona aunque los datos estén cifrados.	**Solo afecta el contenido que coincide con las reglas de bloqueo.** Requiere que los proxy funcionen con páginas web cifradas.	**Afecta elementos web y páginas web individuales.** Requiere que los proxy funcionen con páginas web cifradas.	**Afecta elementos y páginas web en particular.** En general, se aplica a nivel de la URL específica.	**Afecta todo el contenido proporcionado por un nombre de dominio, sea ilegal o no.** No se puede usar de manera eficaz para distribuir contenido.
¿Qué tipo de técnica es?	Bloquea contenido.	Bloquea contenido.	Bloquea contenido.	Desalienta y frustra el acceso.	Desalienta y frustra el acceso.
¿Cuánto daño colateral causa?	Toda acción destinada a grandes servidores tiene una enorme tasa de falsos positivos, ya que se bloquea tanto contenido ilegal como legal.	Según la calidad de las reglas de bloqueo, la tasa de falsos positivos puede oscilar entre muy baja y bastante alta. Escribir buenas reglas es difícil.	La mayor parte del filtrado de URL se basa en servicios comerciales que clasifican el tráfico. En los bloqueos convencionales, puede ser bastante específico, pero en los bloqueos especiales, la tasa de errores es bastante elevada.	La tasa de falsos positivos se considera baja, porque cada bloqueo de página se solicita de manera individual. El problema de las solicitudes ilegítimas ocasiona el bloqueo de información que no corresponde.	Toda acción destinada a los nombres de dominio que usan los grandes servidores tiene una enorme tasa de falsos positivos, ya que se bloquea tanto contenido ilegal como legal. Cuando se usan redes CDN, es ineficaz (o genera un nivel muy alto de falsos positivos).
¿Cuáles son las maneras comunes de eludirlo?	os editores de contenido pueden cambiar las direcciones IP, migrar el contenido o utilizar una CDN para eludirlo. Los usuarios de VPN pueden eludirlo ocultando las direcciones IP.	El uso de múltiples capas de cifrado puede eludir fácilmente este tipo de bloqueo. Cuando las reglas de filtrado no están bien elaboradas, un pequeño cambio en el texto permite sortear los bloqueos con facilidad.	El uso de múltiples capas de cifrado puede eludir fácilmente este tipo de bloqueo. El uso de una capa de aplicación no estándar a menudo es una técnica de evasión eficaz.	Los usuarios pueden elegir muy fácilmente plataformas alternativas, p. ej., un motor de búsqueda diferente.	Los usuarios pueden usar instalaciones locales para evitar las búsquedas de DNS, o enviar sus consultas a un servidor público que no esté modificado (en general, mediante una VPN).
¿Existen efectos secundarios o problemas técnicos?	Mantener largas listas de direcciones IP es un método difícil y proclive a errores, que requiere muchos recursos. Los dispositivos de red que realizan este tipo de bloqueos suelen ser veloces, por lo que no son habituales los problemas de rendimiento.	El filtrado con reconocimiento de contenido tiene grandes costos de rendimiento y es poco práctico en muchos entornos (sin enormes recursos). Cuando se utilizan los proxy, la seguridad puede verse gravemente comprometida.	El filtrado de las URL puede ocasionar problemas de rendimiento y reducir la velocidad y la confiabilidad en general. Cuando se utilizan los proxy, la seguridad puede verse gravemente comprometida.	Muchos motores de búsqueda notifican sobre la información "suprimida", lo que deja un rastro al contenido.	La seguridad del DNS corre riesgos cuando se implementa un servidor modificado.

Conclusión

Comprender las diferentes técnicas de bloqueo así como sus efectos directos e indirectos es importante tanto para los encargados de formular políticas que están considerando tomar estas medidas como para los defensores de Internet y otras personas que desean influir en las prácticas de bloqueo de contenido.

Todas las técnicas de bloqueo tienden a presentar dos desventajas principales:

1. **No resuelven el problema**

   Las técnicas de bloqueo no eliminan el contenido de Internet, no detienen la actividad ilegal ni procesan a los responsables; simplemente colocan una cortina frente al contenido. El contenido subyacente permanece en su lugar.

2. **Ocasionan daños colaterales**

   Cada técnica aplica bloqueos excesivos o insuficientes, es decir, bloquea más de lo deseado y, al mismo tiempo, menos. Las técnicas de bloqueo también causan otros daños, ya que ponen a los usuarios en riesgo (cuando intentan eludir los bloqueos), reducen la transparencia y la confianza en Internet, favorecen la clandestinidad de los servicios e invaden la privacidad de los usuarios. Todos estos costos deben tenerse en cuenta al analizar el bloqueo.

Información adicional:
Cómo evadir el bloqueo de contenido

Los encargados de formular políticas deben tener presente un punto importante al considerar el bloqueo de contenido en Internet: un usuario suficientemente motivado puede eludir todos los métodos técnicos de bloqueo. En muchos casos, solo se requiere un esfuerzo mínimo.

Si se bloquea el tráfico a un host o a un nombre de dominio, se pueden usar herramientas como las VPN para ocultar el tráfico. Si se inspecciona el contenido del tráfico, este se puede cifrar para no activar el bloqueo. Si el contenido se elimina, otros usuarios pueden volver a cargarlo en otros servidores. Si se quita el nombre de dominio utilizado, los usuarios finales pueden acceder al host si conocen la dirección IP, o bien se puede seleccionar un nuevo nombre de dominio para reemplazarlo. Si un motor de búsqueda elimina resultados, siempre habrá otros motores de búsqueda.

Los usuarios finales no son los únicos que pueden eludir los bloqueos (y, de hecho, lo hacen). Los editores de información tienen muchos métodos para eludir diversas técnicas de bloqueo. Si se esfuerzan lo suficiente para distribuir y difundir su contenido, ninguna técnica de bloqueo puede detenerlos.

Recomendaciones

Internet Society (ISOC) cree que la mejor manera de evitar el contenido y las actividades ilegales en Internet es atacarlos en su origen. El uso de filtros para bloquear el acceso al contenido en línea es poco eficaz y tiende a ocasionar daños colaterales para usuarios de Internet que no tienen la culpa.

Queremos sugerir dos estrategias a los encargados de formular políticas preocupados sobre el contenido ilegal en Internet:

1. **Atacar el problema en el origen:** el método menos dañino es "atacar" el contenido y las actividades ilegales en el origen. Eliminar el contenido ilegal del origen y aplicar las leyes contra los infractores evita los efectos negativos del bloqueo y resulta más eficaz para eliminar el contenido ilegal[10]. La cooperación entre actores y jurisdicciones es un requisito esencial para el éxito, ya que el contenido ilegal en línea se extiende más allá de las fronteras y las leyes nacionales.

10 Cuando la autoridad nacional se encuentra en la misma jurisdicción que el consumidor del contenido, eliminar el contenido ilegal en el origen parece una manera fácil de evitar las complejidades y los costos de las acciones internacionales. Sabemos que eliminar el contenido en el origen es complicado en el contexto de una Internet internacional, donde los proveedores y los consumidores del contenido pueden encontrarse en jurisdicciones diferentes y estar sujetos a leyes diferentes. Sin embargo, consideramos que esa no debería ser una razón para no identificar soluciones más eficientes que no perjudiquen a Internet.

2. **Priorizar y utilizar enfoques alternativos:** según las circunstancias, el uso de enfoques diferentes puede ser muy eficaz. Por ejemplo:

    - La cooperación eficaz entre proveedores de servicios, entidades encargadas de la aplicación de la ley y autoridades nacionales puede ofrecer otras maneras de ayudar a las víctimas del contenido ilegal y de tomar medidas coercitivas contra los infractores[11].
    - La creación de un entorno de confianza donde los usuarios reciban información sobre lo que es ilegal y lo que no lo es puede mejorar el autocontrol.
    - En algunos casos (p. ej., en el control parental), facultar al usuario para que utilice filtros en sus propios dispositivos, con su consentimiento, puede ser eficaz y menos dañino para Internet.
    - Algunos sitios web (p. ej., los sitios web de apuestas) pueden utilizar la geolocalización para evitar el acceso desde países donde sus servicios no están permitidos, ya sea de manera voluntaria o porque así lo exige la ley.

Reducción de los efectos negativos al mínimo

Todas las técnicas de bloqueo de contenido son verdaderamente deficientes, especialmente para el bloqueo por razones de políticas públicas. Todas las técnicas tienen defectos y pueden ser evadidas. Por esta y por las razones expresadas anteriormente, desaconsejamos el bloqueo de contenido.

No obstante, estas técnicas se siguen utilizando. Como reconocemos esta realidad, ofrecemos las siguientes pautas específicas para minimizar los efectos negativos:

a. **Descarte todas las opciones que no impliquen bloqueo:** antes que nada, se deben agotar todas las opciones viables para ocuparse del problema del contenido en el origen o para aplicar cualquier otro medio alternativo al bloqueo. No se debe adoptar el bloqueo de contenido simplemente porque es más sencillo.

b. **Sea transparente:** debe existir transparencia respecto al bloqueo y a los objetivos y las políticas subyacentes. Las autoridades nacionales deben asegurarse de que los usuarios afectados tengan la posibilidad de plantear sus preocupaciones por los efectos negativos sobre sus derechos, intereses y oportunidades.

c. **Considere su responsabilidad hacia Internet:** quienes recurren al bloqueo deben ser conscientes de que comparten la responsabilidad de no dañar la estabilidad, la seguridad y la resiliencia de Internet en su conjunto. Las técnicas de bloqueo perjudican el modo en que se administra y funciona colectivamente Internet. El daño a veces es directo y otras veces, indirecto. Por ejemplo, los usuarios que evaden el bloqueo pueden causar problemas o poner en riesgo su seguridad personal.

e. **Piense globalmente, actúe localmente:** el bloqueo y el filtrado local pueden tener efectos globales. Sin embargo, si se bloquea el contenido al nivel más local posible, generalmente se minimiza el impacto global. De manera ideal, el bloqueo en el dispositivo o punto de conexión del usuario es más eficaz y reduce al mínimo los daños colaterales.

f. **Involucre a los actores:** el desarrollo y la implementación de políticas debe involucrar a un amplio grupo de actores, como especialistas en tecnología, economía y derechos de los consumidores, entre otros, para garantizar que se den los pasos adecuados para minimizar los efectos secundarios negativos.

g. **Mantenga el carácter temporal del bloqueo:** todas las medidas deben ser temporales. Se deben eliminar apenas desaparezca la razón del bloqueo. Es bastante habitual que el contenido ilegal cambie de lugar para eludir las medidas de bloqueo, pero que las medidas sigan vigentes mucho después de que el contenido se ha trasladado.

h. **Siga el proceso legal debido:** toda orden de bloquear contenido ilícito debe estar respaldada por la ley, someterse a revisiones independientes y apuntar a una meta muy precisa para alcanzar un objetivo legítimo. Para abordar la actividad ilegal, se debe dar prioridad al medio menos restrictivo que haya disponible. Los proveedores de servicios de Internet u otros intermediarios de Internet no deberían convertirse en agentes de aplicación de la ley de facto: no se les debe exigir que determinen cuándo una conducta o un contenido es ilegal.

11 Por ejemplo, las alianzas con el sector financiero pueden permitir identificar y limitar las transacciones ilegales.

Glosario

CDN Una red de entrega o de distribución de contenido (CDN) es una red de servidores proxy implementados en múltiples centros de datos que se encuentran distribuidos por todo el mundo. El objetivo de una CDN es entregar contenido a los usuarios finales con alta disponibilidad y alto rendimiento. En la actualidad, las CDN proporcionan una fracción importante del contenido de Internet, incluidos los objetos web (texto, gráficos y scripts), los objetos descargables (archivos multimedia, software, documentos), las aplicaciones (de comercio electrónico [e-commerce], portales), el streaming multimedia en vivo, el streaming multimedia a petición y los medios sociales. (https://en.wikipedia.org/wiki/Content_delivery_network)

Contenido En el contexto de este artículo, "contenido" generalmente se utiliza para describir la información que se encuentra en Internet. Puede ser un documento completo o apenas un párrafo de un texto, una imagen, un video o, incluso, solo audio (p. ej., un podcast). El contenido puede encontrarse en páginas web que se visualizan en un navegador, o bien estar disponible a través de herramientas más especializadas, p. ej., en una aplicación personalizada.

DNS El sistema de nombres de dominio (DNS) es un sistema de nomenclatura jerárquico y descentralizado que permite identificar computadoras, servicios u otros recursos conectados a Internet o a una red privada. Asocia diversa información con los nombres de dominio asignados a cada entidad participante. Lo más importante es que traduce los nombres de dominio, que son más fáciles de memorizar, en las direcciones IP numéricas que se necesitan para ubicar e identificar los dispositivos y servicios informáticos con los protocolos de red subyacentes. Al proporcionar un servicio de directorio distribuido a nivel mundial, el sistema de nombres de dominio es un componente esencial para la funcionalidad de Internet y se ha utilizado desde 1985. (https://en.wikipedia.org/wiki/Domain_Name_System)

DPI La inspección profunda de paquetes (DPI, del inglés "Deep Packet Inspection") es una forma de filtrado de paquetes en redes informáticas que analiza los datos (y, posiblemente, también el encabezado) de un paquete al pasar por un punto de inspección, en busca incumplimiento del protocolo, virus, spam, intromisiones u otros criterios definidos para decidir si el paquete puede pasar o si es necesario darle otro tipo de tratamiento, que puede incluir su eliminación. (https://en.wikipedia.org/wiki/Deep_packet_inspection)

Ilegal En el contexto de este artículo, el término "ilegal" se utiliza para describir el contenido que está prohibido en algún ámbito nacional, sea cual fuere el motivo. El contenido puede ser ilegal porque infringe derechos de copyright (u otro tipo de propiedad intelectual), como las películas pirateadas. Puede ser ilegal porque es objetable desde el punto de vista legal, como el contenido obsceno o la pornografía infantil. Puede ser ilegal porque las autoridades nacionales desean suprimirlo o lo consideran ofensivo, como una caricatura que representa de una manera desfavorable al presidente del país. El contenido que es ilegal en una jurisdicción puede ser completamente legal en otra. El contenido que es ilegal en un contexto (por ejemplo, una comedia indecente vista por niños) puede ser completamente legal en otro contexto (por ejemplo, cuando la ven personas adultas), incluso en la misma jurisdicción.

Dirección IP Una dirección IP (abreviatura de dirección de Protocolo de Internet) es un identificador asignado a cada equipo y dispositivo (p. ej., impresoras, enrutadores, dispositivos móviles, etc.) conectado a Internet. Se utiliza para ubicar e identificar un nodo en las comunicaciones con otros nodos de la red. (https://en.wikipedia.org/wiki/IP_address)

Falso negativo Un falso negativo se produce cuando no se bloquea contenido que debería haberse bloqueado. Por ejemplo, si se bloquean las farmacias ilegales, es posible que una farmacia ilegal recién creada no se bloquee si el servidor donde reside aún no se ha agregado a la lista de direcciones bloqueadas. Esto se denomina "falso negativo".

Falso positivo Un falso positivo se produce cuando se bloquea contenido que no se intentaba bloquear. Por ejemplo, si se bloquea la pornografía, pero el bloqueo utiliza una búsqueda de palabras claves mal elaborada, podrían bloquearse las recetas para cocinar pechugas de pollo. Esto se consideraría un falso positivo.

TLS/SSL La seguridad de la capa de transporte (TLS) y su antecesora, la capa de sockets seguros (SSL), ambas denominadas frecuentemente "SSL", son protocolos de cifrado que proporcionan seguridad para las comunicaciones en una red de computadoras. Existe un uso extensivo de varias versiones de los protocolos en aplicaciones como navegadores web, correo electrónico, fax por Internet, mensajería instantánea y voz sobre IP (VoIP). Los sitios web utilizan TLS para proteger todas las comunicaciones entre sus servidores y los navegadores web. El principal objetivo del protocolo de seguridad de la capa de transporte es la privacidad y la integridad de los datos entre dos aplicaciones informáticas que se comunican. (https://en.wikipedia.org/wiki/Transport_Layer_Security)

URL La dirección del localizador uniforme de recursos (URL), llamada "dirección web" de manera informal, es una referencia a un recurso web que indica su ubicación en la red y un mecanismo para recuperarlo. Las URL por lo general se utilizan para hacer referencia a páginas web (https), pero también se utilizan para transferencia de archivos (ftp), correo electrónico (mailto), acceso a bases de datos (JDBC) y muchas otras aplicaciones. La mayoría de los navegadores web muestran la URL de una página web en una barra de direcciones situada arriba de la página. Una dirección URL típica puede tener el formato https://www.ejemplo.com/muestra.html, que indica un protocolo (https), un nombre de host (www.ejemplo.com) y un nombre de archivo (muestra.html). (https://en.wikipedia.org/wiki/Uniform_Resource_Locator)

VPN Una red privada virtual (VPN) extiende una red privada sobre una red pública, como Internet. Permite a los usuarios enviar y recibir datos a través de redes públicas o compartidas como si sus dispositivos estuviesen conectados directamente a la red privada. Por consiguiente, las aplicaciones que se ejecuten en la VPN pueden beneficiarse de la funcionalidad, la seguridad y la administración de una red privada. (https://en.wikipedia.org/wiki/Virtual_private_network)

Lecturas adicionales

Las siguientes publicaciones pueden ser de interés para los lectores que desean obtener información adicional acerca de este tema.

Documentos técnicos del Grupo de Trabajo de Ingeniería de Internet (IETF)

"A Survey of Worldwide Censorship Techniques" (Encuesta mundial de técnicas de censura) (IETF draft draft-hall-censorship-tech-04)
Ωhttps://tools.ietf.org/html/draft-hall-censorship-tech-04

"Technical Considerations for Internet Service Blocking and Filtering" (Consideraciones técnicas para el bloqueo y el filtrado de servicios de Internet) (RFC 7754)
https://tools.ietf.org/html/rfc7754

Documentos sobre políticas, encuestas y antecedentes

"Filtering, blocking and take-down of illegal content on the Internet" (Filtrado, bloqueo y eliminación de contenido ilegal en Internet), Consejo de Europa, 2015.
http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

"Freedom of Expression Unfiltered: How blocking and filtering affect free speech" (Libertad de expresión sin filtros: cómo el bloqueo y el filtrado afectan la libre expresión), Article 19, 2016.
https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

"Freedom on the Net 2016" (Libertad en la red 2016), Freedom House, noviembre de 2016.
https://freedomhouse.org/report/freedom-net/freedom-net-2016

"Perspectiva de Internet Society sobre el filtrado de sistemas de nombres de dominios (DNS)", Internet Society, 2012.
https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf

"Neutralidad de la red", Internet Society, 2015.
http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030.pdf

"Perspectives on Policy Responses to Online Copyright Infringement" (Perspectivas sobre las respuestas políticas a la violación de derechos de autor en línea), Internet Society, 2011.
https://www.internetsociety.org/sites/default/files/bp-copyrightpolicy-20110220-en-1.pdf

Reconocimientos

Internet Society reconoce con gratitud la asistencia de Joel Snyder de Opus One para la preparación de este artículo.

El informe fue supervisado por Nicolas Seidler y Andrei Robachevsky de Internet Society.

Asimismo, se benefició de las revisiones, los comentarios y el apoyo del personal de 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.

Agradecemos especialmente al equipo de Comunicaciones de Internet Society por elaborar la presentación visual del trabajo y por promover su lanzamiento: James Wood, Beth Gombala, Lia Kiessling, Allesandra Desantillana.

Por último, aunque no por eso menos importante, este artículo mejoró significativamente gracias a los aportes de diversos miembros de los Capítulos, representantes de organizaciones, miembros individuales y miembros del Consejo de Administración de Internet Society.

Internet Society

internetsociety.org

Galerie Jean-Malbuisson 15,
CH–1204 Ginebra, Suiza
Tel. +41 22 807 1444

1775 Wiehle Avenue, Suite 201
Reston, Virginia 20190, EE. UU.
Tel. +1 703 439 2120