Internet Society — Perspectivas sobre o bloqueio de conteúdo na Internet: visão geral

Março de 2017

Internet Society

Sumário

Prefácio

O uso de bloqueio da Internet por governos, para impedir o acesso a conteúdos ilegais é uma tendência crescente no mundo inteiro. Os legisladores podem apresentar muitos motivos para o bloqueio do acesso a algum conteúdo, como jogos on-line, propriedade intelectual, proteção das crianças e segurança nacional. No entanto, exceto por problemas relacionados a pornografia infantil, há pouco consenso internacional sobre o que constitui conteúdo apropriado, sob uma perspectiva de ordem pública.

O objetivo deste documento é fornecer uma avaliação técnica dos diferentes métodos de bloqueio de conteúdo da Internet, incluindo como cada método funciona e quais são as armadilhas e os problemas associados a cada um. Não pretendemos analisar a legalidade ou as motivações políticas do bloqueio de conteúdo da Internet[1].

Nossa conclusão, baseada em análises técnicas, é que o uso do bloqueio da Internet para lidar com conteúdos ou atividades ilegais costuma ser ineficiente, muitas vezes é ineficaz, e na maior parte do tempo causa danos involuntários aos usuários da Internet.

Do ponto de vista técnico, é recomendável que os legisladores pensem duas vezes ao considerarem o uso de ferramentas de bloqueio da Internet para resolverem questões de ordem pública. Se pensarem realmente e optarem por utilizar abordagens alternativas, esta será uma importante conquista para uma Internet global, aberta, interoperável e confiável.

1 Leitores interessados em análises jurídicas do bloqueio de conteúdo podem acessar os recursos a seguir:
- Artigo 19: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf
- Conselho Europeu: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-Internet

Introdução

A evolução da Internet em um fenômeno social em todo o mundo deve muito ao conteúdo e serviços que aproveitam a arquitetura única da rede mundial. Economias inteiras dependem dos fluxos de conteúdo entre fronteiras. Inovações diárias têm o potencial para perturbar setores inteiros. Atualmente, a Internet representa uma parte fundamental dos processos democráticos e das discussões políticas. As pessoas criam e rompem relacionamentos on-line.

A tendência não está diminuindo. De acordo com estimativas[2], Em 2020, o tráfego global da Internet será equivalente a 95 vezes o volume de toda a Internet global em 2005. O número de dispositivos conectados a redes IP será três vezes mais alto que a população mundial em 2020.

Ainda assim, a Internet também contém conteúdo que decisores políticos, legisladores e autoridades reguladoras do mundo inteiro desejam bloquear. No caso do bloqueio de sites de apostas estrangeiros na Europa e América do Norte ou do bloqueio de discursos políticos na China, o uso de técnicas de bloqueio de conteúdo na Internet para impedir o acesso a conteúdo considerado ilegal sob certas leis nacionais é um fenômeno global. Motivações de ordem pública para o bloqueio de conteúdo na Internet são bastante diversificadas, abrangendo combate à violação da propriedade intelectual, materiais ligados ao abuso infantil e atividades ilegais on-line, bem como proteção da segurança nacional.

O objetivo deste documento não é avaliar tais motivações nem qualificar determinado tipo de bloqueio como bom ou mau sob uma perspectiva ética, legal, econômica, política ou social. Em vez disso, nossa intenção é fornecer uma avaliação técnica das vantagens e desvantagens das técnicas de bloqueio mais comuns utilizadas para impedir o acesso a conteúdo considerado ilegal. O objetivo é ajudar os leitores a entender o que cada técnica pode e não pode bloquear, além dos efeitos colaterais, armadilhas, negociações de meios-termos e custos associados.

Nossa conclusão é que o uso do bloqueio da Internet para lidar com conteúdo ilegal costuma ser ineficiente, muitas vezes ineficaz, e tende a causar danos colaterais indesejados aos usuários da Internet, resumidos na tabela da página 6.

Do ponto de vista técnico, **apelamos aos decisores para que** pensem duas vezes sobre o uso de tais medidas e solicitamos que priorizem suas respostas com foco principalmente em medidas alternativas que visem enfrentar o problema na origem (veja recomendações mais detalhadas no fim deste documento, incluindo orientações sobre como minimizar os efeitos negativos de tais medidas.).

Observe-se ainda que este documento não pretende abordar medidas de bloqueio implantadas para o gerenciamento normal de redes ou por motivos de segurança (por ex., lidar com spam e malware). Nesses casos, algumas das mesmas ferramentas descritas neste documento geralmente são eficazes para os objetivos pretendidos.

Barra lateral:
Filtragem, bloqueio ou censura?

Quando descrevemos a filtragem na Internet, termos como “filtragem”, “bloqueio”, “suspensão” e “censura” nos vêm à mente (assim como vários outros). Do ponto de vista do usuário, o termo selecionado é menos importante que o efeito: alguma parte da Internet está inacessível. para decisores e ativistas digitais, a escolha de determinado termo geralmente é guiada mais pelos sobretons semânticos que pela correção técnica. A palavra “censura” traz em si forte conotação negativa, enquanto “filtragem” parece uma operação mais suave e inofensiva, como remover sementes indesejadas de um copo de suco de laranja. Optamos por utilizar “bloqueio” como um termo simples e claro, ao longo de todo este documento.

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

A tabela abaixo resume as principais dificuldades associadas ao bloqueio de conteúdo da Internet com base em considerações de ordem pública:

Problema	Detalhes
Facilmente evitado	Todas as técnicas descritas neste documento podem ser evitadas por usuários suficientemente motivados. À medida que os usuários descobrem as diferentes maneiras de contornar o bloqueio, a eficácia deste é reduzida.
Não resolve o problema	O bloqueio do conteúdo não remove o conteúdo considerado ilegal. Em alguns casos, uma proibição nacional pode ser incompatível com as normas internacionais, mas onde há um amplo acordo sobre conteúdo ilegal, a melhor solução para o problema é a remoção do conteúdo na origem.
Causa danos colaterais	Quando conteúdos legais e ilegais compartilham o mesmo endereço IP, nome de domínio ou outras características, o bloqueio do conteúdo bloqueará o acesso a tudo, seja legal ou ilegal. Por exemplo, o bloqueio do acesso a um único artigo da Wikipédia usando filtragem de DNS também bloquearia milhões de outros artigos do site.
Põe os usuários em risco	Quando o serviço de Internet local não é considerado confiável e aberto, os usuários da Internet podem usar abordagens alternativas e fora do padrão, como download de software que redireciona o tráfego para evitar filtros. Essas soluções improvisadas sujeitam os usuários a riscos de segurança adicionais.
Incentiva a falta de transparência	Um ambiente transparente e confiável é importante para o bom funcionamento da Internet. O bloqueio do conteúdo elimina a transparência, minando a natureza aberta da rede e causando desconfiança nas fontes de informações públicas.
Direciona o serviço para camadas mais profundas	Quando o bloqueio de conteúdo torna-se generalizado, serviços "subterrâneos" e estruturas alternativas de sobreposição da rede são estabelecidos, tirando o conteúdo das vistas das autoridades. Por exemplo, o conteúdo pode mover-se para a Internet obscura (Dark Web) ou os usuários podem criar um tráfego em túnel por meio de VPNs.
Invade a privacidade	Vários tipos de bloqueio de conteúdo exigem a análise de tráfego do usuário, incluindo o tráfego criptografado. A violação da privacidade ocorre quando terceiros monitoram o que os usuários da Internet fazem, registram transações ou violam a segurança de criptografia básica da Internet.
Gera preocupações com os direitos humanos e com o devido processo	Implementado sem a devida consideração por noções como necessidade e proporcionalidade, o bloqueio de conteúdo tem o potencial para causar danos colaterais significativos, restrição das comunicações livres e abertas, e limitação dos direitos dos indivíduos.

Motivações para o bloqueio de conteúdo

Neste documento, abordamos o **bloqueio baseado em considerações de ordem pública** e seus efeitos sobre a Internet e seus usuários (veja a barra lateral para conhecer outras motivações para o bloqueio de conteúdo).

O bloqueio baseado em considerações de ordem pública é utilizado por autoridades nacionais para restringir o acesso a informações (ou a serviços relacionados) consideradas ilegais em determinada jurisdição, vistas como ameaça à ordem pública ou censuráveis para determinado público.

Por exemplo, a maioria dos países deseja bloquear o acesso de crianças a materiais obscenos, ou o acesso por qualquer pessoa a materiais de abuso infantil. Dependendo do ambiente jurídico local, o conteúdo também poderá ser bloqueado se violar as leis de propriedade intelectual, se for considerado uma ameaça à segurança nacional ou proibido por razões culturais ou políticas.

Um dos desafios que levam autoridades nacionais a utilizar medidas de bloqueio de conteúdo na Internet é que diferentes atores que entregam conteúdo da origem aos consumidores podem estar em diferentes países, com diferentes leis que definem o que é ou não "conteúdo ilegal". Além disso, o ambiente global da Internet torna o impedimento da fonte de conteúdo ilegal mais complicado do que simplesmente desativar um servidor local. Por exemplo, a pessoa que fornece o conteúdo, os servidores que o hospedam e, por fim, o nome de domínio que aponta para o conteúdo podem estar em países distintos, fora do alcance da jurisdição de uma autoridade individual nacional. Isso ressalta a importância da cooperação entre jurisdições e a necessidade de uma coordenação direta com as partes interessadas não governamentais.

Outros tipos de motivações para o bloqueio de conteúdo

Nosso foco, neste documento, está no bloqueio baseado em considerações de ordem pública, mas existem duas outras razões comuns para bloqueios na rede. A primeira é **prevenir ou responder a ameaças à segurança da rede**. Este tipo de bloqueio é muito comum. Por exemplo, a maioria das empresas tenta bloquear o ingresso de malware em suas redes. Muitos provedores de serviços de Internet (ISPs) implantam bloqueios para tráfego mal-intencionado que sai de suas redes, como dispositivos IoT sequestrados (p.ex., webcams). A filtragem de e-mail é extremamente comum e inclui o bloqueio de e-mail em massa indesejado, bem como de e-mail mal-intencionado, como mensagens de phishing. Esses tipos de bloqueio não são descritos neste documento.

Um segundo motivo para o bloqueio é o **gerenciamento de uso da rede**. Uma área crescente de bloqueio de conteúdo da Internet se baseia em requisitos de gerenciamento da rede, da largura de banda ou do tempo, em vez de em determinados tipos de conteúdo. Por exemplo, empregadores podem limitar o acesso a sites de redes sociais de seus funcionários, sem retirarem o acesso à Internet em computadores. Os ISPs podem bloquear ou permitir, regular ou acelerar certos conteúdos, com base nos serviços contratados. O gerenciamento da utilização da rede raramente é uma questão de ordem pública, exceto quando se sobrepõe à área do comportamento anticompetitivo. Leitores interessados em neutralidade da rede poderão encontrar materiais de consulta em Leituras adicionais, na página 26.

Visão geral das técnicas de bloqueio de conteúdo

Cada técnica apresenta limitações tanto técnicas quanto políticas, além de consequências que precisam ser consideradas quando é proposto qualquer tipo de bloqueio de conteúdo. O objetivo deste documento é fornecer um modo comum de analisar sua eficácia e efeitos colaterais. Leitores interessados em uma discussão mais técnica sobre o bloqueio de conteúdo encontrarão referências aos documentos técnicos da IETF em Para leituras adicionais, na página 26.

Este documento avaliará os seguintes tipos de bloqueio de conteúdo:

- Bloqueio baseado em IP e protocolo
- Bloqueio baseado em inspeção profunda de pacotes
- Bloqueio baseado em URL
- Bloqueio baseado em plataforma (especialmente mecanismos de busca)
- Bloqueio baseado em DNS

Selecionamos esses cinco tipos de bloqueio porque são direcionados aos elementos de um ciclo de descoberta e recuperação de informações de um usuário final típico, incluindo o uso de um mecanismo de busca e visualização de informações com um navegador da web ou ferramenta semelhante. Esse ciclo é muito familiar aos decisores políticos, eles próprios usuários da Internet, e essas são as operações que tentam ser interrompidas pela maioria dos bloqueios baseados em considerações de ordem pública.

No diagrama à direita, apresentamos as etapas que um usuário típico da Internet poderia assumir para encontrar informações, além dos tipos de bloqueios que têm sido utilizados para interromper o ciclo quando é implantado o bloqueio baseado em considerações de ordem pública. No nosso diagrama, um usuário da Internet pesquisa algum tipo de conteúdo utilizando um mecanismo de busca (etapa 1), um ponto de partida comum. O mecanismo de busca retorna um conjunto de resultados (etapa 2), e o usuário clica em um deles após selecioná-lo (etapa 3). Um tipo de bloqueio, baseado na plataforma, é utilizado para interromper esta parte do ciclo, bloqueando alguns resultados gerados pelo mecanismo de busca.

O computador do usuário tenta localizar o servidor que hospeda os dados no DNS da Internet (etapas 4 e 5). Um segundo tipo de bloqueio, baseado no DNS, é utilizado para interromper esta parte do ciclo.

Em seguida, o navegador do usuário tenta se conectar ao servidor (etapa 6). Essa parte do ciclo pode ser bloqueada com o uso de três outros tipos de bloqueio: bloqueio baseado em IP e protocolo, bloqueio baseado em URL e bloqueio baseado em inspeção profunda de pacotes.

Visão geral: etapas da recuperação e bloqueio de informações on-line

1. Um usuário pesquisa a palavra "bomba" usando um mecanismo de busca.
2. Sem filtragem, o usuário vê um resultado
3. O usuário clica em um resultado (http://exemplo.com/bomba)
4. O computador do usuário analisa "exemplo.com" no DNS para poder se conectar ao servidor web.
   - exemplo.com? → DNS → RESOLVEDOR
5. exemplo.com = 192.0.222
6. O navegador da web conecta-se ao servidor web "exemplo.com" e solicita a página da web específica em que o usuário clicou.
   - **Para:** 192.0.222
   - **Solicitação do PC do usuário para o servidor exemplo.com**
   - **Obter:** http://exemplo.com/bomba
7. **De:** 192.0.222
   - **Solicitação do servidor de exemplo.com para o usuário**
   - **Obter:**

Se estiver ocorrendo bloqueio, isto será exibido:

Com a **filtragem de pesquisa** e outros bloqueios baseados na plataforma, os resultados sairão do controle do usuário se ele utilizar determinado mecanismo de busca.	Com o **bloqueio baseado em DNS,** o computador do usuário não conseguirá encontrar o servidor; portanto, não conseguirá se conectar à página da web. Será exibido "Servidor não encontrado".	Com o **bloqueio baseado em IP e protocolo,** a conexão ao servidor com IP = 192.0.222 é bloqueada. Todo o conteúdo do servidor fica indisponível, intencionalmente ou não.	Com o **bloqueio baseado em URL**, o tráfego é bloqueado quando o URL está na lista de bloqueio.	Com o **bloqueio baseado em inspeção profunda de pacotes (Deep Packet Inspection),** palavras-chave na página da web podem ativar uma interrupção do tráfego. Há alto risco de bloqueio involuntário de conteúdo.
Nenhum resultado para "bomba"	**Servidor não encontrado**	**A conexão expirou**	**Este site foi bloqueado pelo administrador da rede**	**A conexão foi redefinida**

Obviamente, a Internet é muito mais que pesquisas e navegadores, e muitas das técnicas discutidas abaixo são eficazes para o bloqueio de mais do que páginas da web. Por exemplo, geralmente é possível bloquear a utilização de serviços VPN para criptografar e ocultar o tráfego com uma combinação de bloqueio por inspeção profunda de pacotes e bloqueio baseado em IP/protocolo.

Esses tipos de bloqueio podem ser aplicados de forma muito específica (a um determinado documento em determinado site), ou muito genericamente (a "material sobre um assunto" ou "serviços de voz sobre IP").

Onde ocorre o bloqueio de conteúdo?

Muitas das técnicas de bloqueio de conteúdo discutidas aqui podem ser utilizadas em diferentes pontos, como vemos na tabela abaixo.

Nível nacional	Quando exigido por políticas governamentais, todo o tráfego que ingressa ou sai de um país pode estar sujeito a bloqueio de conteúdo. Isso requer rígido controle de todas as conexões entre fronteiras, por meio de um gateway ou firewall nacional, ou pode ser imposto a todas as operadoras e ISPs em um país em paralelo.
Nível de operadora e ISP	Operadoras individuais de telecomunicações, incluindo operadoras de telefonia móvel e ISPs tradicionais, podem instalar ferramentas de bloqueio.
Nível de rede local	O laptop e os computadores de mesa do usuário final geralmente estão conectados a redes domésticas, corporativas ou de instituições de ensino, em vez de diretamente a uma operadora. Essas redes locais podem ter bloqueios instalados, geralmente baseados em gerenciamento de rede ou políticas de segurança, e não em políticas governamentais.
Nível de ponto de extremidade	Um software capaz de aplicar a política de bloqueio pode ser instalado diretamente nos computadores de usuários finais. Este método é muito utilizado em redes domésticas e corporativas, geralmente por razões de segurança, mas também para gerenciamento da rede ou controle parental.

Observe que, no caso de bloqueio com base em considerações de políticas públicas, a maioria das medidas é aplicada nos dois primeiros níveis (operadora nacional e provedor).

O diagrama abaixo resume alguns dos principais locais onde é possível haver bloqueio, assim como os tipos de bloqueio que podem ocorrer em cada ponto.

O bloqueio de conteúdo da Internet pode ocorrer em muitos pontos

Barra lateral:
Bloqueio de conteúdo no ponto de extremidade

Este documento aborda o bloqueio de conteúdo na Internet com base em considerações de ordem pública.

Ainda assim, é importante observar que um dos modos mais eficazes de bloquear conteúdo indesejado é pelo uso de software instalado no dispositivo do usuário, geralmente chamado de "ponto de extremidade", porque é o último ponto da conexão entre o usuário e a Internet. A maioria dos usuários de computadores utiliza software de ponto de extremidade para bloquear malware (vírus, cavalos de troia e phishing), independentemente de serem instalados pessoalmente ou pelo grupo de TI de uma empresa.

O software de bloqueio de conteúdo em ponto de extremidade também é utilizado por organizações para o bloqueio de conteúdo por outros motivos. Por exemplo, bibliotecas normalmente instalam esse tipo de aplicativo em computadores públicos para bloquearem a visualização de pornografia por clientes, e os pais podem utilizá-lo para bloquear conteúdo que seus filhos não devem visualizar.

O bloqueio de conteúdo no ponto de extremidade pode utilizar muitas das técnicas descritas neste documento, incluindo varredura de conteúdo, categorização de URL, bloqueio por endereço IP e interceptação do DNS. Em geral, o bloqueio e a análise ocorrem no ponto de extremidade real. Entretanto, fornecedores desses aplicativos começam a utilizar, cada vez mais, ferramentas baseadas em nuvem, incluindo varredura de conteúdo e bloqueio baseado no DNS, juntamente com alguma colaboração de software de ponto de extremidade. Nas soluções mais recentes, parte ou todo o conteúdo da Internet pode passar por um serviço baseado em nuvem. A vantagem de mover a tomada de decisão para a nuvem é que os pontos de extremidade não precisam ser atualizados constantemente, e o impacto sobre o desempenho da avaliação de conteúdo é transferido do computador ou do smartphone do usuário para uma nuvem de computadores facilmente escalável. Contudo, quando o tráfego é direcionado por terceiros, isso também cria problemas de privacidade ao tornar o conteúdo disponível para esses terceiros e, quando a implantação é deficiente, também podem ocorrer problemas de segurança.

Avaliação de tipos de bloqueio de conteúdo

Os cinco tipos comuns de bloqueio de conteúdo se diferenciam em termos do que bloqueiam e de como operam.

A seguir, discutimos as técnicas de bloqueio de conteúdo em maiores detalhes e as avaliamos em relação a quatro critérios específicos[3].

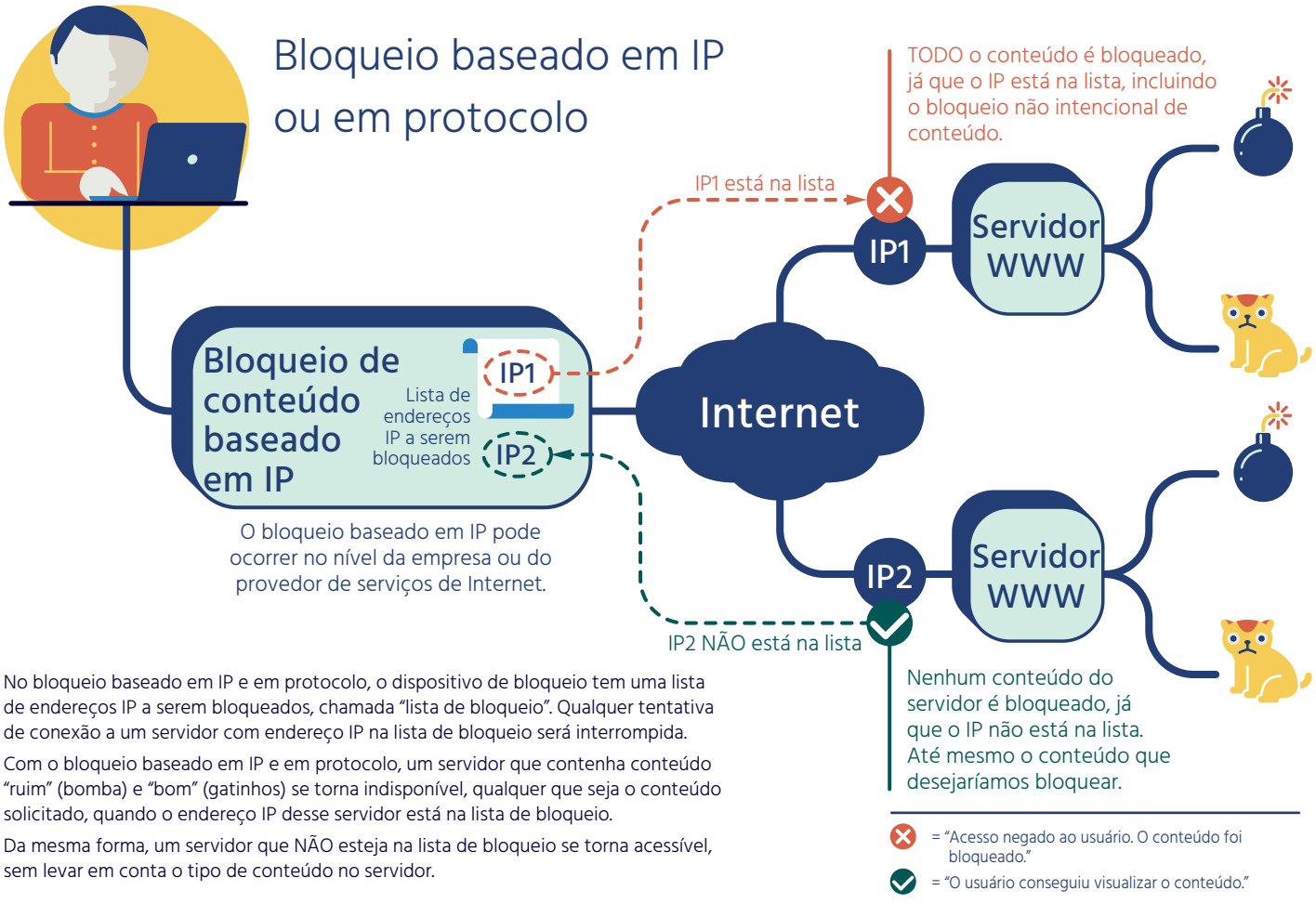
1. **Que conjuntos de usuários e serviços de Internet são afetados por esta técnica?** Que conjuntos não são afetados?
2. **Até que ponto essa técnica é específica para impedir o acesso a determinado conteúdo?** Quanto dano colateral (bloqueio involuntário) pode ser gerado pela técnica de bloqueio?
3. **Até que ponto a técnica é eficaz para o bloqueio de conteúdo?** Que tipos de usuários e provedores de conteúdo conseguiriam contornar essa técnica?
4. **Quais são os efeitos colaterais comuns dessa técnica?** Que problemas técnicos podem ser causados por essa técnica? Que questões não técnicas, como impacto na confiança e direitos fundamentais, podem surgir com o uso dessa técnica?

3 Estes critérios foram retirados da RFC (Solicitação de Comentários) 7754 para a Internet, "Considerações técnicas para bloqueio e filtragem de serviços de Internet."

Bloqueio baseado em IP e em protocolo

O bloqueio baseado em IP impõe barreiras na rede, como firewalls, que bloqueiam todo o tráfego como um conjunto de endereços IP. O bloqueio baseado em protocolo utiliza outros identificadores de rede de baixo nível, como número de porta TCP/IP, que podem identificar determinado aplicativo em um servidor ou um tipo de protocolo de aplicativo. Estas abordagens mais simples ao bloqueio de conteúdo não bloqueiam diretamente o conteúdo, mas sim o tráfego para endereços IP ou portas TCP/IP conhecidas, ou protocolos associados a algum conteúdo ou aplicativo. O bloqueio baseado em IP ou protocolo também pode ser feito por software em computadores de usuários, geralmente para fins de segurança da rede.

Por exemplo, se o objetivo fosse bloquear todo o conteúdo hospedado no país fictício Elbônia, o bloqueio por IP poderia ser utilizado se fosse conhecido o conjunto de todos os endereços IP que hospedam conteúdo em Elbônia. Similarmente, se o objetivo fosse bloquear todos os serviços de VPN (usados para criptografar o tráfego e ocultar o destino e o conteúdo), o bloqueio baseado em protocolo poderia ser usado para impedir que os serviços de VPN usassem protocolos conhecidos ou números de portas TCP/IP.



No bloqueio baseado em IP e em protocolo, o dispositivo de bloqueio tem uma lista de endereços IP a serem bloqueados, chamada "lista de bloqueio". Qualquer tentativa de conexão a um servidor com endereço IP na lista de bloqueio será interrompida.

Com o bloqueio baseado em IP e em protocolo, um servidor que contenha conteúdo "ruim" (bomba) e "bom" (gatinhos) se torna indisponível, qualquer que seja o conteúdo solicitado, quando o endereço IP desse servidor está na lista de bloqueio.

Da mesma forma, um servidor que NÃO esteja na lista de bloqueio se torna acessível, sem levar em conta o tipo de conteúdo no servidor.

Uma variação do bloqueio por IP é o controle do tráfego. Neste cenário, nem todo o tráfego é bloqueado, o que ocorre apenas com determinada porcentagem dele. Os usuários podem perceber que o serviço está muito lento, ou que simplesmente "vai e vem". Isso pode ser usado para desencorajar o uso de um serviço por usuários, fazendo com que não pareça confiável, ou para encorajar o uso de serviços alternativos, sem revelar a ocorrência do bloqueio. (outro objetivo também pode ser o gerenciamento da rede e da largura de banda nos níveis de ISP ou da empresa).

Os bloqueios por IP e por protocolo utilizam dispositivos localizados entre o usuário final e o conteúdo e, portanto, exigem que o responsável pelo bloqueio (por exemplo, o ISP do usuário) tenha controle completo sobre a conexão entre o usuário final e a Internet. Um usuário que não está "atrás" do dispositivo de bloqueio, ou que utiliza tecnologia como VPN, que oculta o real destino do tráfego, não será afetado por este tipo de bloqueio.

Em geral, o bloqueio do IP não é uma técnica de filtragem muito eficaz, pois é difícil de manter com eficiência, tem alto nível de bloqueio adicional não pretendido, e pode ser facilmente evitado por editores que movem o conteúdo para novos servidores (com novos endereços IP).

O bloqueio por IP também não funciona quando os provedores de informações utilizam redes de entrega de conteúdo (CDNs), já que os endereços IP das informações são altamente dinâmicos e mudam constantemente.[4] CDNs também utilizam o mesmo endereço IP para muitos clientes e tipos de conteúdo, causando um alto nível de interrupção involuntária do serviço.

O bloqueio por IP e por protocolo funciona melhor quando utilizado para bloquear aplicativos específicos, em vez de conteúdo específico. Por exemplo, o tráfego VPN pode ser bloqueado por bloqueios de porta TCP/IP e de protocolo, combinados com bloqueio de endereço IP de serviços VPN públicos conhecidos. Esta é uma técnica comum e altamente eficaz.

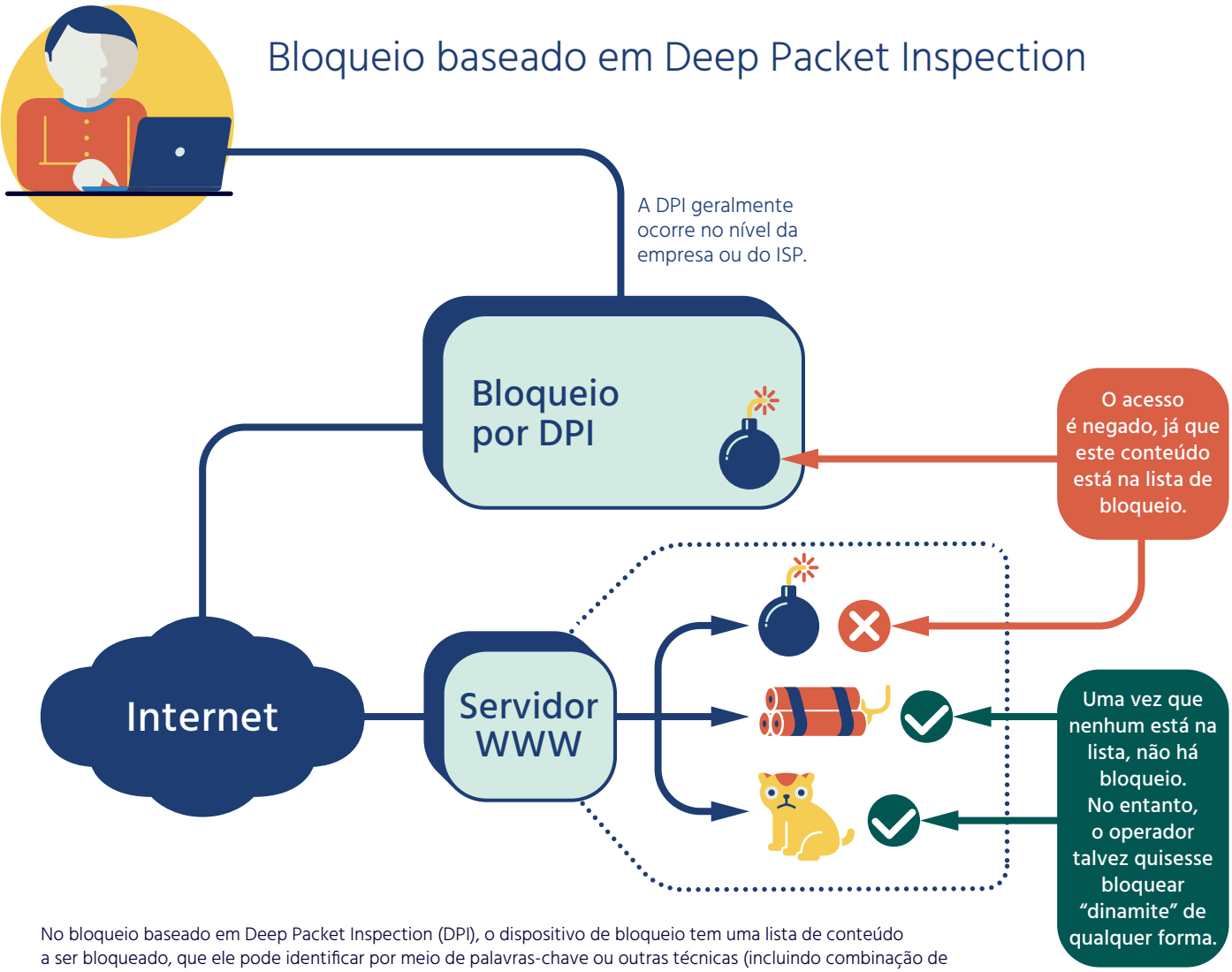
O bloqueio por IP também é mais eficaz quando o conteúdo está hospedado em determinado servidor em um data center específico, ou quando há preocupação com um conjunto muito específico de dados. O bloqueio baseado em IP **não** é muito eficaz para serviços de hospedagem mais amplos distribuídos entre vários data centers, ou que utilizam redes de distribuição de conteúdo (CDNs) para acelerar o acesso.

4 Uma rede de distribuição de conteúdo é uma ampla rede de servidores dispersos geograficamente que aceleram a entrega de conteúdo da web para usuários da Internet. Grandes CDNs têm centenas de milhares de servidores em muitos países, para fornecerem acesso mais rápido ao conteúdo de seus clientes. CDNs armazenam cópias de conteúdo de texto, imagem, áudio e vídeo de seus clientes em seus próprios servidores, nas proximidades das "bordas" da Internet, de modo que as solicitações dos usuários possam ser atendidas por um servidor edge, em vez de pelos servidores centralizados do cliente.

Bloqueio baseado em Deep Packet Inspection

O bloqueio baseado em Deep Packet Inspection (DPI) utiliza dispositivos entre o usuário final e o restante da Internet que filtram com base em conteúdo, padrões ou tipos de aplicativos específicos. Este tipo de bloqueio de rede é muito intensivo em termos de computação e, portanto, é caro, pois todo o conteúdo deve ser analisado em relação às regras de bloqueio. O bloqueio por DPI também pode ser feito por software em computadores de usuários, geralmente para fins de segurança da rede.

Para ser eficaz, esse bloqueio requer algum tipo de assinatura ou informações sobre o conteúdo. As informações podem ser palavras-chave, características do tráfego (por exemplo, tamanhos de pacote ou taxas de transmissão), nomes de arquivos ou outras informações específicas do conteúdo. O bloqueio por DPI é usado com muita eficácia para bloquear ou controlar certos aplicativos (por exemplo, compartilhamento de arquivos ponto a ponto ou tráfego de voz sobre IP [VoIP]) e tipos de arquivos de dados (por exemplo, arquivos multimídia).



No bloqueio baseado em Deep Packet Inspection (DPI), o dispositivo de bloqueio tem uma lista de conteúdo a ser bloqueado, que ele pode identificar por meio de palavras-chave ou outras técnicas (incluindo combinação de imagens). Será interrompida qualquer tentativa de baixar conteúdo não criptografado que corresponda à lista.

Com a DPI, falsos positivos (bloqueio incorreto de conteúdo) e falsos negativos (falha em bloquear o conteúdo pretendido) são comuns. Também é difícil executar a DPI quando o tráfego é criptografado.

Neste diagrama, "bomba" foi bloqueada porque corresponde ao conteúdo. No entanto, dinamite não estava bloqueada, mesmo se o operador do dispositivo de DPI desejasse bloqueá-la, pois dinamite não correspondia à lista de bloqueio de conteúdo.

O bloqueio por DPI é usado com muita frequência em empresas para sistemas de proteção contra vazamento de dados, produtos antimalware (antivírus) e gerenciamento de rede para priorização do tráfego (p.ex., aumentar a prioridade de videoconferência corporativa). No entanto, também pode ser usado para fins de bloqueio mais baseado em políticas. Por exemplo, o uso dos serviços de VoIP não fornecidos pela operadora nacional de telecomunicações geralmente é controlado e restrito, e o bloqueio por DPI é eficaz para impor essas restrições.

O bloqueio por DPI usa dispositivos localizados entre o usuário final e o conteúdo e, portanto, o responsável pelo bloqueio (por exemplo, o ISP do usuário) deve ter controle completo sobre a conexão entre o usuário final e a Internet. Quando o tráfego é criptografado, como ocorre com frequência, os sistemas de bloqueio por DPI podem deixar de ser eficazes. Tudo isso é abordado em maiores detalhes na barra lateral "Criptografia, proxies e desafios ao bloqueio", à direita.

A técnica de bloqueio por DPI geralmente é eficaz para o bloqueio de certos tipos de conteúdo que podem ser identificados por meio de assinaturas ou outras regras (por exemplo, "bloquear todo o tráfego de Voz sobre IP"). O bloqueio por DPI tem sucesso muito menor com outros tipos de conteúdo, como determinados arquivos ou documentos multimídia com certas palavras-chave incluídas. Como o bloqueio por DPI examina todo o tráfego para usuários finais, ele é bastante invasivo em termos da privacidade do usuário final.

A eficácia total do bloqueio por DPI varia muito, dependendo dos objetivos e das ferramentas de DPI específicas utilizadas. Em geral, as ferramentas de DPI são mais eficazes no gerenciamento de redes e na aplicação de segurança, e não são muito adequadas para bloqueio baseado em políticas.

Barra lateral:
Criptografia, proxies e desafios ao bloqueio

Várias técnicas abordadas neste documento, incluindo bloqueio baseado em inspeção profunda de pacotes (DPI) e bloqueio baseado em URL, têm uma limitação muito real: elas devem ser capazes de ver o tráfego que pretendem analisar. Servidores da web que oferecem criptografia ou usuários que adicionam criptografia às suas comunicações (geralmente por tecnologia de criptografia específica ao aplicativo, como TLS/SSL) não podem ser bloqueados de modo confiável por dispositivos na rede. Muitas das outras técnicas também são facilmente contornáveis quando o usuário tem acesso a tecnologia de VPN, que criptografa as comunicações e oculta o real destino e tipo de tráfego. Embora pesquisadores e fornecedores tenham desenvolvido algumas formas de identificar determinados tipos de tráfego por inferência e análise, geralmente essas técnicas são apenas palpites sobre o tipo de tráfego.

Em uma pesquisa recente, 49% do tráfego da web nos EUA (por volume) era criptografado, em fevereiro de 2016. (Ver: http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf) Este tráfego seria efetivamente invisível para o bloqueio baseado em URL e por ferramentas de DPI que analisam o conteúdo, porque a única informação visível seria o nome do domínio do servidor que hospeda a informação. Para compensar essa "ocultação de informações", alguns bloqueios de rede utilizam dispositivos ativos (chamados de proxies) que interceptam e descriptografam o tráfego entre o usuário e o servidor web, rompendo o modelo de criptografia ponta a ponta de TLS/SSL.

O uso de proxies causa preocupações significativas sobre a segurança e a privacidade. Com a ruptura do modelo TLS/SSL, quem realiza o bloqueio obtém acesso a todos os dados criptografados e pode, inadvertidamente, permitir que terceiros façam o mesmo. O proxy também pode alterar o conteúdo. Se o responsável pelo bloqueio tiver controle sobre o sistema do usuário (por exemplo, um dispositivo gerenciado por uma empresa seria altamente controlado), o proxy poderá ser muito transparente. Em geral, contudo, a presença de um proxy seria óbvia para o usuário final, pelo menos para tráfego criptografado (TLS/SSL) (p.ex., o usuário pode ver um aviso de que o certificado não vem de uma autoridade confiável). Além disso, novos padrões do setor e IETF (como a Segurança de Transporte Estrita de HTTP [RFC6797], Pinning de Chave Pública de HTTP [RFC 7469], e DANE [RFC 6698]) e novos recursos de segurança em navegadores modernos dificultam fazer proxy (e descriptografar) o tráfego TLS/SSL sem conhecimento e cooperação do usuário final.

Proxies instalados para o bloqueio de conteúdo também podem introduzir gargalos de desempenho no fluxo de tráfego da rede, tornando os serviços lentos ou não confiáveis.

Bloqueio baseado em URL

O bloqueio baseado em URL é um método muito popular de bloqueio e pode ocorrer tanto no computador individual quanto em um dispositivo de rede entre o computador e o restante da Internet. O bloqueio por URL funciona com aplicativos baseados na web e não é utilizado para o bloqueio de aplicativos não web, como VoIP. Com o bloqueio por URL, um filtro intercepta o fluxo de tráfego da web (HTTP) e verifica o URL, que aparece na solicitação HTTP, em relação a um banco de dados local ou serviço on-line. Com base na resposta, o filtro de URL permitirá ou bloqueará a conexão com o servidor web solicitado.

Em geral, os URLs são gerenciados por categorias (por exemplo, "sites de esportes") e toda uma categoria é bloqueada, controlada ou permitida[5]. No caso de uma política nacional que exija bloqueio de URL, o serviço on-line e a política de bloqueio provavelmente serão gerenciados pelo governo. O filtro de URL pode simplesmente interromper o tráfego, ou redirecionar o usuário para outra página da web, mostrando uma declaração da política ou observando que o tráfego foi bloqueado. O bloqueio de URL na rede pode ser executado por proxies, assim como por firewalls e roteadores.

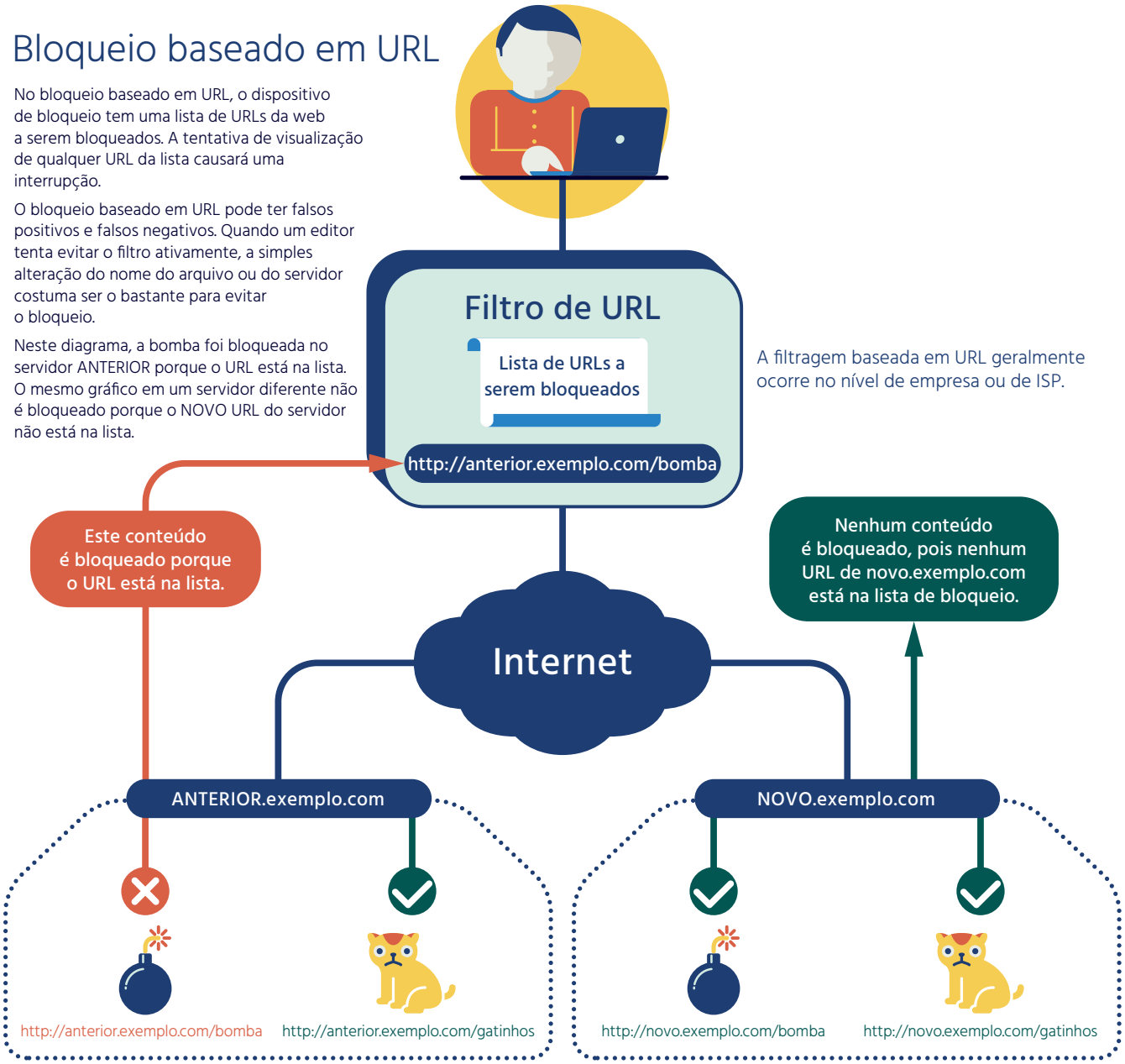
5 Categorias de filtragem por URL são estabelecidas por provedores de serviços de segurança e geralmente se baseiam em uma combinação de análise humana de páginas da web e alguma varredura automática de conteúdo de páginas da web. A maioria dos provedores de serviços de segurança oferece bancos de dados de filtragem de URLs para fins de gerenciamento do tráfego de redes corporativas, mas eles podem ser usados em outros contextos, como aqueles descritos neste documento.

Bloqueio baseado em URL

No bloqueio baseado em URL, o dispositivo de bloqueio tem uma lista de URLs da web a serem bloqueados. A tentativa de visualização de qualquer URL da lista causará uma interrupção.

O bloqueio baseado em URL pode ter falsos positivos e falsos negativos. Quando um editor tenta evitar o filtro ativamente, a simples alteração do nome do arquivo ou do servidor costuma ser o bastante para evitar o bloqueio.

Neste diagrama, a bomba foi bloqueada no servidor ANTERIOR porque o URL está na lista. O mesmo gráfico em um servidor diferente não é bloqueado porque o NOVO URL do servidor não está na lista.



Esse bloqueio requer que o responsável pelo bloqueio (como o ISP do usuário) tenha a capacidade de interceptar e controlar o tráfego entre o usuário final e a Internet. Geralmente é caro, porque o dispositivo de filtragem normalmente precisa estar em linha entre o usuário e a Internet e, portanto, exige um alto nível de recursos para um desempenho aceitável.

A eficácia do bloqueio de URL geralmente é muito alta para identificar o conteúdo que pode estar em diferentes servidores ou serviços, porque o URL não muda, mesmo que o servidor altere os endereços IP. Em alguns casos, o bloqueio de URL pode não bloquear totalmente o tráfego, quando os URLs são muito complicados ou mudam com frequência. Isso pode ocorrer porque um editor de informações decidiu evitar, de modo deliberado e ativo, o bloqueio por filtragem de URL, ou este pode ser um efeito colateral de alguns sistemas avançados de edição, como aqueles utilizados para grandes publicações on-line.

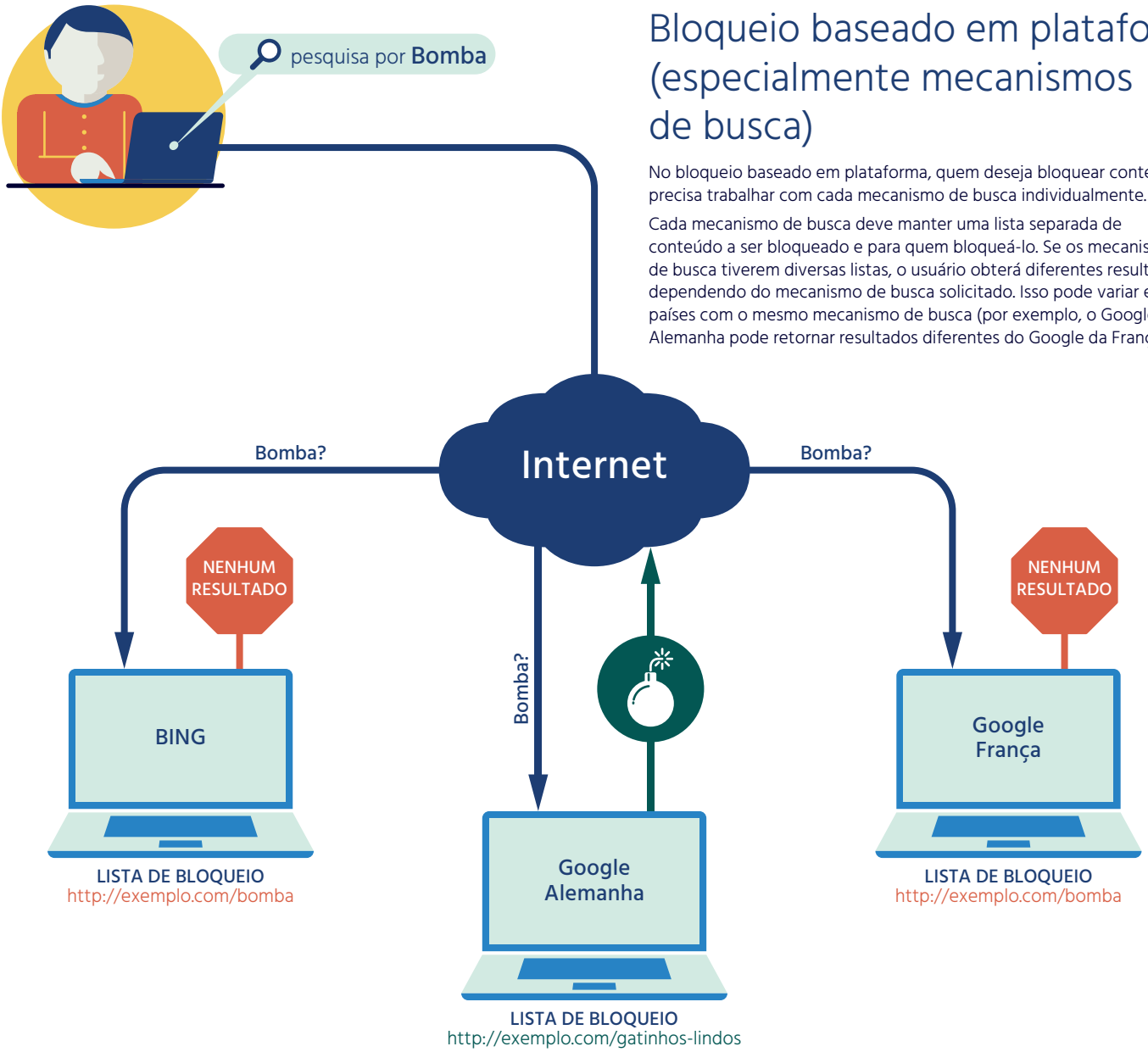
O bloqueio de URL geralmente é eficaz em URLs de alto nível, como uma página da web específica, mas não é tão eficaz quando links profundos (como bits individuais de conteúdo em uma página da web) são considerados. Dependendo de como o usuário navegou até o conteúdo específico, o bloqueio de URL pode ou não ser capaz de bloquear totalmente o acesso. Se o usuário tiver um "deep link" não coberto pelo filtro de URL, o conteúdo será permitido. Por exemplo, o site da Playboy inclui o URL playboy.com, mas também apresenta conteúdo integrado que utiliza o nome de domínio "playboy.tv". Um filtro de URL que não incluiu também "playboy.tv" não bloqueará o conteúdo de vídeo.

Todos os tipos de bloqueio de URL dependem muito da qualidade do filtro, e um filtro mal planejado ou excessivamente amplo pode bloquear tráfego não pretendido ou ter outros efeitos negativos sobre a experiência do usuário, como afetar o carregamento ou formatação de páginas da web quando algum componente está sendo bloqueado.

Como ocorre com tipos de bloqueio por inspeção profunda de pacotes, o bloqueio de URL requer que algum tipo de proxy veja o URL completo quando o tráfego está criptografado com HTTPS (TLS/SSL). Veja a barra lateral "Criptografia, Proxies e Desafios ao Bloqueio", na página 15, para obter mais informações sobre os efeitos sobre a privacidade do usuário final. Para tráfego criptografado, o bloqueio de URL pode ver apenas o endereço IP do servidor, e não o URL completo, resultando em um nível muito superior de bloqueio involuntário. Como proxies são caros e invasivos à experiência do usuário, o bloqueio de URL não funciona bem como ferramenta para bloqueio baseado em política.

Bloqueio baseado em plataforma (especialmente mecanismos de busca)

Em alguns casos, as autoridades nacionais trabalharão com grandes provedores de serviços de informações para bloquear informações dentro de sua região geográfica sem o bloqueio de toda a plataforma. Os tipos mais comuns de filtragem de plataforma ocorrem por meio de grandes provedores de mecanismos de buscas e plataformas de mídia social. Recentemente, também foi relatado que lojas de aplicativos móveis (como Apple Store e Google Play) estão trabalhando com autoridades nacionais para bloquear downloads de aplicativos específicos em seu país.



Bloqueio baseado em plataforma (especialmente mecanismos de busca)

No bloqueio baseado em plataforma, quem deseja bloquear conteúdo precisa trabalhar com cada mecanismo de busca individualmente.

Cada mecanismo de busca deve manter uma lista separada de conteúdo a ser bloqueado e para quem bloqueá-lo. Se os mecanismos de busca tiverem diversas listas, o usuário obterá diferentes resultados, dependendo do mecanismo de busca solicitado. Isso pode variar entre países com o mesmo mecanismo de busca (por exemplo, o Google da Alemanha pode retornar resultados diferentes do Google da França).

O bloqueio baseado em plataforma é uma técnica que requer a assistência do proprietário da plataforma, como um operador de mecanismo de busca como Google ou Microsoft. Nessa técnica, consultas de um determinado conjunto de usuários da Internet a um mecanismo de busca receberão um conjunto de resultados diferentes do restante da Internet — com filtragem de indicadores para conteúdo que seja censurável de alguma forma. Em alguns casos, a definição do que deve ser bloqueado baseia-se em regulamentos locais e exigências do governo, mas também pode se dever a preocupações do operador do mecanismo de busca. Por exemplo, um mecanismo de busca pode bloquear apontadores para malware ou conteúdo considerados inapropriados de acordo com seus próprios termos de serviço.

Como o bloqueio pelo mecanismo de busca requer a cooperação do provedor do mecanismo de busca, sua utilização fica limitada a dois cenários muito específicos: regras de nível nacional (bloqueio de conteúdo com base em regras específicas de cada país ou região) e regras baseadas em idade (bloqueio de material inadequado para jovens).

O bloqueio de mecanismos de pesquisa só afeta usuários que escolhem determinado mecanismo de busca e somente quando eles são identificados como pertencendo a determinado conjunto com regras de filtragem. No bloqueio baseado em idade, como o SafeSearch,[6] (oferecido pelos principais mecanismos de busca e provedores de conteúdo), é preciso haver a opção de aceitar o recurso.

Como o bloqueio do mecanismo de busca só filtra apontadores para o conteúdo, não o conteúdo em si, esta técnica é extremamente ineficaz, e pode ter a consequência não pretendida de atrair maior atenção para o conteúdo bloqueado. A presença de vários mecanismos de busca, bem como métodos alternativos de encontrar conteúdo, tornam a aplicação deste tipo de bloqueio muito difícil.

Embora o bloqueio de mecanismos de busca pareça fazer muito pouco no sentido de bloquear conteúdo, a técnica é extremamente popular em nível nacional, e governos do mundo inteiro já exigiram que grandes mecanismos de busca implantassem filtros de acordo com seus regulamentos, como para a violação de direitos autorais ou determinados tipos de discursos proibidos por leis nacionais. Em 2015, por exemplo, o Google informou que havia recebido 8.398 solicitações de 74 tribunais nacionais para remover 36.834 resultados de seus resultados de pesquisa[7]. Solicitações por violação de direitos autorais feitas por pessoas físicas também são muito populares: em junho de 2016, o Google informou que 6.937 proprietários de direitos autorais haviam solicitado a remoção de mais de 86 milhões de resultados de pesquisa dos resultados do Google naquele mês[8].

O bloqueio de mecanismos de busca também é usado por pessoas físicas como parte do chamado "direito de ser esquecido", com a solicitação de bloqueio de mais de um milhão de URLs no mundo inteiro nos últimos dois anos (de maio de 2014 a junho de 2016).

Barra lateral:
Bloqueio em outras plataformas

Embora o bloqueio em mecanismo de busca seja o tipo mais comum de bloqueio de plataforma, outras plataformas com enormes comunidades de usuários são muitas vezes consideradas para essa técnica. Exemplos comuns desses tipos de plataformas incluem Facebook (com mais de 1,5 bilhões de usuários ativos a cada mês) e YouTube (com mais de um bilhão de usuários únicos). É muito difícil utilizar técnicas baseadas na rede ou em URL para bloquear elementos individuais de conteúdo, como determinadas publicações. Para que não sejam vistas como censoras de todo o Facebook (por exemplo), autoridades de alguns países propuseram trabalhar com grandes fornecedores de plataformas para filtrarem tipos específicos de conteúdo que consideram ilegais.

Sabemos muito pouco sobre a eficácia, o escopo ou os efeitos colaterais de outros tipos de bloqueio por plataforma, já que esta técnica não tem sido observada de forma ampla e confiável em plataformas que não sejam as de mecanismos de busca. Embora grandes plataformas, como Facebook, YouTube e Twitter, bloqueiem de forma geral certos tipos de conteúdo (como malware e materiais pornográficos) e ofereçam feeds de conteúdo personalizados aos seus usuários, informações sobre bloqueios específicos a certos países não estão disponíveis.

6 O SafeSearch é um recurso de grandes mecanismos de pesquisa, incluindo Google Search, Microsoft Bing e Yahoo!que bloqueia os resultados que contêm "imagens inadequadas ou explícitas" dos resultados de pesquisa.

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

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

Bloqueio de conteúdo baseado em DNS

O bloqueio de conteúdo baseado em DNS evita um dos problemas presentes nas outras técnicas: o custo e impacto sobre o desempenho da filtragem de todo o tráfego da rede. Em vez disso, o bloqueio de conteúdo baseado em DNS tem seu foco no exame e controle de consultas ao DNS.

Nesse tipo de bloqueio, um resolvedor especializado do DNS (veja a Barra Lateral: Visão Geral do DNS) tem duas funções: além de executar buscas no DNS, o resolvedor verifica os nomes, comparando-os com uma lista de bloqueio. Quando o computador de um usuário tenta utilizar um nome bloqueado, o servidor retorna informações incorretas, como o endereço IP de um servidor que exibe um aviso informando que o conteúdo foi bloqueado. Ou, ainda, o servidor pode declarar que o nome não existe. O efeito é que o usuário é impedido de acessar facilmente o conteúdo utilizando certos nomes de domínio.

Como ocorre com o bloqueio de conteúdo baseado em toda a rede, o bloqueio de conteúdo baseado em DNS é eficaz apenas quando a organização que realiza o bloqueio tem completo controle sobre a conexão de rede do usuário final. Se o usuário puder selecionar uma conexão diferente ou utilizar outro conjunto de servidores do DNS, a técnica não o afetará. Por exemplo, quando a Turquia bloqueou algumas consultas ao DNS em 2012, os usuários mudaram seus sistemas para utilizar servidores DNS públicos e populares do Google e evitar o bloqueio. Autoridades turcas responderam com o sequestro de todo o tráfego para o serviço DNS do Google, o que causou danos secundários significativos. O bloqueio de conteúdo baseado no DNS requer firewalls ou outros dispositivos capazes de interceptar e redirecionar todas as consultas do DNS para os servidores DNS especializados e usados para o bloqueio, ou este não será muito eficaz.

A eficácia do bloqueio de conteúdo baseado no DNS é semelhante ao bloqueio baseado em IP. Ele é ligeiramente mais eficaz, porque a lista de nomes de domínio é mais fácil de atualizar e é mais precisa que uma lista de endereços IP para a maioria dos tipos de bloqueio de conteúdo. Entretanto, ele é ligeiramente menos eficaz, pois mudar nomes de domínio é mais simples que alterar endereços IP, o que facilita a evasão deste tipo de bloqueio por usuários finais e editores de informações.

Uma forma alternativa de bloqueio de conteúdo baseado no DNS ocorre quando nomes de domínio são retirados ou removidos totalmente do DNS. Este método é mais difícil de contornar e o dano secundário é limitado. Em muitos casos, isso depende da eficácia da cooperação transfronteiriça, quando uma solicitação ou ordem judicial vêm de uma jurisdição diferente daquela onde opera o registro ou agente de registro.

O bloqueio de conteúdo baseado no DNS apresenta desvantagens semelhantes ao bloqueio com base no endereço IP: conteúdo proibido e não proibido podem estar no mesmo servidor que utiliza o mesmo nome (p.ex., "facebook.com"), mas tudo seria bloqueado. Além disso, a modificação das respostas do DNS pode causar outros problemas técnicos que interrompam outros serviços válidos[9].

O bloqueio de conteúdo baseado no DNS também depende de os usuários obedecerem as regras normais da Internet e usarem o serviço DNS padrão para a conversão de nomes em endereços IP. Os usuários que têm controle total sobre seus próprios computadores e algum conhecimento técnico podem reconfigurá-los para contornar o serviço padrão do DNS e usar alternativas, ou simplesmente terem uma lista de conversões de nomes em endereços armazenada localmente.

Barra lateral:
Visão geral do DNS

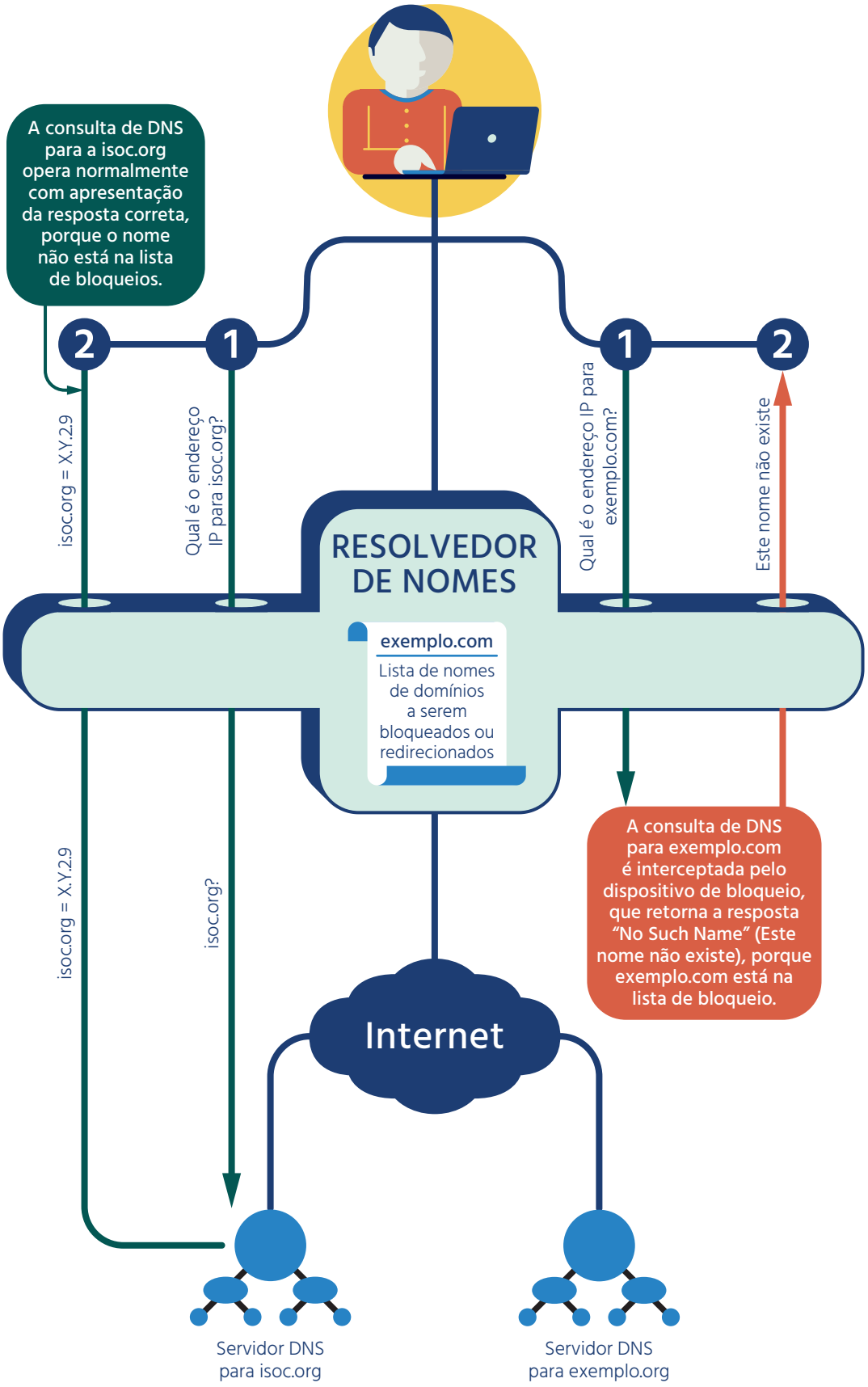
O DNS é um sistema conceitualmente simples, que permite que uma cadeia de rótulos (como "www", "isoc" e "org") separada por pontos (o nome do domínio) seja analisada em um banco de dados distribuído entre vários servidores DNS. A consulta do nome de domínio resulta em uma resposta (por exemplo, um endereço IP ou site), ou na resposta de que o nome não existe.

O tipo mais comum de consulta DNS se refere a endereços IP (Internet Protocol). Esse é o tipo de consulta que ocorre sempre que, por exemplo, um usuário digita um URL em um navegador. Normalmente, o aplicativo individual (como o navegado) não executa a consulta completa, que envolve várias etapas. Em vez disso, o aplicativo utiliza um sistema intermediário, chamado "resolvedor" (porque resolve as buscas de nomes DNS), que percorre o banco de dados distribuído do DNS para recuperar a informação solicitada.

No bloqueio de conteúdo do DNS, a operação normal do resolvedor é diferente.

9 Leitores interessados em mais detalhes podem consultar o relatório "Perspectives on DNS Filtering" (Perspectivas sobre a Filtragem no DNS) da Internet Society em https://www.Internetsociety.org/Internet-society-perspectives-domain-name-system-dns-filtering-0

Bloqueio baseado em DNS



No bloqueio baseado em DNS, o dispositivo de bloqueio tem uma lista de nomes DNS a serem bloqueados.

Como a maioria das conexões de Internet requer conversão de um nome de DNS em um endereço IP, o bloqueio da consulta e retorno de uma resposta falsa podem desestimular os usuários de tentar recuperar o conteúdo bloqueado ou se conectar com serviços bloqueados por outros meios (por exemplo, diretamente, digitando o endereço IP).

Resumo do bloqueio de conteúdo

Técnicas de bloqueio de conteúdo na Internet					
	Bloqueio baseado em IP e em protocolo	**Bloqueio baseado em inspeção profunda de pacotes**	**Bloqueio baseado em URL**	**Bloqueio baseado em plataforma (especialmente mecanismos de busca)**	**Bloqueio baseado em DNS**
Visão Geral	Um dispositivo inserido na rede realiza o bloqueio com base no endereço IP e/ou aplicativo (p.ex., VPN).	Um dispositivo inserido na rede realiza o bloqueio com base em palavras-chave e/ou outro conteúdo (nome de arquivo, por exemplo).	Um dispositivo inserido na rede intercepta solicitações da web e analisa URLs comparando-os com uma lista de bloqueio.	Trabalhando com fornecedores de aplicativos (como mecanismos de busca), o conteúdo é modificado de acordo com as exigências locais.	No nível de rede ou de ISP, o tráfego do DNS é encaminhado para um servidor modificado do DNS, que pode bloquear consultas de certos nomes de domínio.
É eficaz?	Como endereços IP podem ser alterados e o conteúdo pode ser modificado facilmente, **essa técnica é bastante falha**. Ela funciona bem apenas quando o editor de informações não se empenha ativamente para contornar o bloqueio.	Quando as informações bloqueadas são caracterizadas facilmente, ela é muito efetiva. Para bloqueio geral (p.ex., "bloqueio de conteúdo adulto") ou quando há criptografia, **a técnica é bastante ineficaz**.	Essa é uma técnica comum que **funciona bem quando o bloqueio ao acesso ocorre para categorias inteiras** de informações. Novas páginas e sites menores podem escapar facilmente, assim como servidores web criptografados.	Uma vez que não há monopólio em mecanismos de busca (por exemplo), e as preferências dos consumidores mudam constantemente, **esse tipo de bloqueio é amplamente cosmético e muito pouco eficiente**.	O bloqueio do DNS é facilmente contornado por editores de conteúdo e usuários finais. O bloqueio do DNS é eficaz apenas quando cada nome tem muito pouco conteúdo, e todo esse conteúdo precisa ser bloqueado. **Desafios técnicos, bloqueio excessivo e facilidade de evasão tornam a técnica ineficaz.**
Quem é afetado?	Qualquer um que esteja "atrás" do dispositivo é afetado.	Qualquer um que esteja "atrás" do dispositivo é afetado.	Usuários "atrás" do dispositivo, e para os quais o dispositivo pode interceptar e avaliar o tráfego da web.	Usuários do mecanismo de busca que instalaram o bloqueio.	Usuários do servidor DNS modificado. Isso pode ser aplicado no nível da rede ou do provedor de serviços.
Até que ponto é específico?	**Afeta todo o conteúdo em um servidor, ilegal ou não.** Funciona mesmo quando os dados são criptografados.	**Afeta apenas o conteúdo que corresponde às regras de bloqueio.** Exige que os proxies operem com páginas da web criptografadas.	**Afeta páginas individuais da web e elementos da web.** Exige que os proxies operem com páginas da web criptografadas.	**Afeta páginas individuais e elementos da web.** Geralmente executado no nível de URL.	**Afeta todo o conteúdo fornecido por um nome de domínio, ilegal ou não.** Não pode ser utilizado com eficácia para distribuir conteúdo.
Que tipo de técnica é essa?	Bloqueia conteúdo.	Bloqueia conteúdo.	Bloqueia conteúdo.	Desencoraja e frustra o acesso.	Desencoraja e frustra o acesso.
Quanto dano secundário pode ocorrer?	Qualquer bloqueio que tenha como alvo servidores maiores apresenta uma imensa taxa de falsos positivos, bloqueando conteúdo tanto ilegal quanto legal.	Dependendo da qualidade das regras de bloqueio, a taxa de falsos positivos pode variar de muito baixa a muito alta. É difícil criar boas regras.	A maior parte da filtragem de URL se baseia em serviços comerciais que categorizam o tráfego. Para bloqueios gerais, a especificidade é grande, mas para bloqueios com fins especiais a taxa de erro é bastante alta.	A taxa de falsos positivos é considerada baixa, porque cada bloqueio de página é solicitado individualmente. O problema de solicitações não legítimas causa o bloqueio de algumas informações inadequadas.	Qualquer bloqueio que tenha como alvo nomes de domínio utilizados por servidores maiores tem uma imensa taxa de falsos positivos, bloqueando conteúdo tanto ilegal quanto legal. Ineficaz com o uso de CDNs (ou resulta em um nível extremamente alto de falsos positivos).
Quais são as formas comuns de evasão?	Os editores podem alterar endereços IP, migrar o conteúdo ou utilizar Redes de Entrega de Conteúdo (CDNs) para contornar o bloqueio. Usuários de VPNs podem contornar o bloqueio ocultando seus endereços IP.	Várias camadas de criptografia contornam com eficácia esse tipo de bloqueio. Quando as regras de filtragem são mal escritas, pequenas mudanças no texto podem contornar facilmente os bloqueios.	Várias camadas de criptografia contornam com eficácia esse tipo de bloqueio. O uso de uma camada de aplicativo não padrão geralmente é uma técnica de evasão eficiente.	Os usuários podem escolher, com muita facilidade, plataformas alternativas, como um mecanismo de busca diferente.	Os usuários podem evitar usar buscas de DNS, usando instalações locais, ou podem enviar suas consultas a um servidor público não modificado (geralmente por uma VPN).
Existem efeitos secundários ou problemas técnicos?	A manutenção de longas listas de endereços IP é difícil e propensa a erros, exigindo recursos significativos. Dispositivos de rede que realizam esse tipo de bloqueio geralmente são rápidos, portanto, problemas de desempenho não são comuns.	A filtragem com especificidade para o conteúdo apresenta custos significativos de desempenho e não é prática em muitos ambientes (sem a implantação de recursos enormes). Quando proxies são usados, a segurança pode ser gravemente comprometida.	A filtragem por URL pode causar problemas de desempenho, reduzindo a velocidade e a confiabilidade geral. Quando proxies são usados, a segurança pode ser gravemente comprometida.	Muitos mecanismos de busca relatam sobre informações "suprimidas", o que em si mesmo cria uma trilha para o conteúdo.	A segurança do DNS é comprometida com a utilização de um servidor modificado.

Conclusão

A compreensão de diferentes técnicas de bloqueio, seus efeitos e efeitos colaterais é importante para decisores que estejam considerando o uso de tais medidas e para defensores da Internet e outros que queiram influenciar as práticas de bloqueio de conteúdo.

Todas as técnicas de bloqueio são suscetíveis a dois problemas principais:

1. **Não resolvem o problema**

   Técnicas de bloqueio não removem o conteúdo da Internet, nem impedem atividades ilegais ou processam os culpados; elas simplesmente ocultam o conteúdo com uma cortina. O conteúdo subjacente permanece no mesmo lugar.

2. **Elas infligem danos colaterais**

   Todas as técnicas de bloqueio sofrem de excessos e insuficiências: bloqueiam além do pretendido e, ao mesmo tempo, menos do que deveriam. Elas também causam outros danos à Internet, ao colocarem os usuários em risco (enquanto tentam contornar os bloqueios), reduzindo a transparência e a confiança na Internet, levando os serviços ao "subterrâneo" e invadindo a privacidade dos usuários. Estes custos devem ser considerados quando discutimos técnicas de bloqueio.

Barra lateral:
Contornar o bloqueio de conteúdo

Decisores devem sempre lembrar de algo muito importante, ao considerarem o bloqueio do conteúdo da Internet: todos os métodos de bloqueio técnico podem ser contornados por um usuário suficientemente motivado. Em muitos casos, o esforço necessário é mínimo para fugir de um bloqueio.

Se o bloqueio for no tráfego para um host ou nome de domínio, ferramentas como VPNs poderão ser utilizadas para ocultar o tráfego. Se o conteúdo do tráfego estiver sendo inspecionado, ele poderá ser criptografado para não ativar o bloqueio. Se o conteúdo for removido, outros usuários poderão migrá-lo para outros servidores. Se o nome de domínio utilizado for removido, usuários finais ainda poderão acessar o host se conhecerem o endereço IP, ou um novo nome de domínio poderá ser selecionado como substituto. Se um mecanismo de busca remover resultados, outros mecanismos de busca poderão ser utilizados.

Usuários finais não são os únicos que podem contornar bloqueios. Editores de informações também têm muitas abordagens para evitar diferentes técnicas de bloqueio. Se um editor se esforçar o suficiente para distribuir e disseminar conteúdo, nenhuma técnica de bloqueio poderá impedi-lo.

Recomendações

A Internet Society acredita que o modo mais apropriado de combater conteúdo e atividades ilegais na Internet é atacando-os na origem. O uso de filtros que bloqueiam o acesso ao conteúdo on-line é ineficiente, provavelmente é ineficaz e tende a gerar danos secundários que afetam usuários inocentes da Internet.

Sugerimos duas estratégias principais para os responsáveis políticos preocupados com conteúdos ilegais na Internet:

1. **Atacar o problema na origem:** a abordagem menos prejudicial para a Internet é "atacar" o conteúdo e as atividades ilegais em sua origem. A remoção do conteúdo ilegal de sua origem e a execução de ações contra os perpetradores evitam os efeitos negativos do bloqueio e são mais eficazes para a remoção de conteúdo ilegal[10]. A cooperação entre jurisdições e partes interessadas é um pré-requisito para o sucesso, já que o conteúdo ilegal on-line estende-se além das fronteiras e das leis dos países.

10 Quando uma autoridade nacional está na mesma jurisdição que o consumidor do conteúdo, a remoção do conteúdo ilegal na origem parece um modo fácil de resolver as complexidades e o custo de ações interfronteiriças. Reconhecemos que remover o conteúdo na origem é difícil no contexto de uma Internet sem fronteiras, onde os provedores e os consumidores de conteúdo podem estar localizados em diferentes jurisdições, sujeitos a diferentes legislações. Ainda assim, consideramos que isso não deve ser um motivo para não identificarmos soluções mais eficientes, que não prejudiquem a Internet.

2. **Priorizar e utilizar abordagens alternativas:** dependendo das circunstâncias, diferentes abordagens podem ser bastante eficazes. Por exemplo:

    - A cooperação efetiva entre provedores de serviço, repressão ao crime e autoridades nacionais pode fornecer meios adicionais de ajudar as vítimas de conteúdo ilegal e de aplicar medidas legais contra os perpetradores[11].
    - A criação de um ambiente de confiança, em que os usuários recebam informações sobre o que é legal ou não, pode melhorar o autopoliciamento.
    - Em alguns casos (p.ex., controle parental), a capacitação do usuário para utilizar filtros em seus dispositivos, com seu consentimento, pode ser mais eficiente e menos prejudicial para a Internet.
    - De modo voluntário ou exigido por lei, alguns sites (p.ex., de jogos on-line) poderiam utilizar a geolocalização para impedir o acesso por países em que seus serviços não são permitidos.

Minimizar efeitos negativos

Todas as técnicas de bloqueio de conteúdo têm graves deficiências, especialmente no contexto do bloqueio com base em considerações de ordem pública. Todas as técnicas são imperfeitas e podem ser contornadas. Por esse motivo e por aqueles já mencionados, orientamos contra o bloqueio de conteúdo.

No entanto, essas técnicas ainda são usadas. Reconhecendo esta realidade, oferecemos as seguintes diretrizes específicas para diminuir o impacto negativo:

a. **Esgote todas as opções que não sejam de bloqueio:** em primeiro lugar, e acima de tudo, esgote opções práticas para abordar o conteúdo na origem ou quaisquer métodos alternativos ao bloqueio. Não se deve tentar bloquear o conteúdo apenas porque é o mais fácil a fazer.

b. **Seja transparente:** deve haver transparência sobre o bloqueio, bem como sobre o objetivo e as políticas subjacentes. As autoridades nacionais devem se certificar de que os usuários afetados tenham a oportunidade de manifestar suas preocupações sobre os impactos negativos aos seus direitos, interesses e oportunidades.

c. **Considere sua responsabilidade com a Internet:** quem bloqueia deve estar ciente de que compartilha a responsabilidade para com o sistema como um todo de não prejudicar a estabilidade, segurança e resiliência da Internet. As técnicas de bloqueio afetam negativamente as funções e o gerenciamento coletivo da Internet. Às vezes, o dano é direto, e às vezes, indireto. Por exemplo, usuários que tentam contornar o bloqueio podem causar problemas ou ameaçar sua segurança pessoal.

e. **Pense globalmente, aja localmente:** o bloqueio e a filtragem locais podem ter efeitos globais. Entretanto, em termos gerais, o bloqueio de conteúdo da forma mais local possível pode minimizar o impacto global. Idealmente, bloquear o ponto de extremidade de um usuário é mais eficaz e minimiza os danos colaterais.

f. **Envolva as partes interessadas:** o desenvolvimento e a implantação de políticas devem envolver um amplo conjunto de interessados, incluindo especialistas em tecnologia, economia, direitos dos consumidores e outros, para garantir a adoção das etapas apropriadas para minimizar efeitos secundários negativos.

g. **Torne temporária a medida:** quaisquer medidas de bloqueio devem ser temporárias. Elas devem ser removidas logo que o motivo para o bloqueio deixar de existir. É bastante comum mover o conteúdo ilegal para contornar medidas de bloqueio, mas as medidas geralmente permanecem em efeito muito tempo após a movimentação do conteúdo.

h. **Siga o processo legal:** qualquer ordem de bloqueio de conteúdo ilegal deve ser respaldada pela lei, analisada de forma independente e estritamente orientada para alcançar um objetivo legítimo. Deve-se dar prioridade aos meios menos restritivos para lidar com a atividade ilegal. Prestadores de serviços de Internet ou outros intermediários da Internet não devem substituir os agentes oficiais de aplicação da lei: eles não devem ser obrigados a determinar quando a conduta ou o conteúdo é ilegal.

11 Por exemplo, parcerias com o setor financeiro podem ser usadas para identificar e limitar transações ilícitas.

Glossário

CDN Uma rede de entrega de conteúdo ou rede de distribuição de conteúdo (CDN) é uma rede globalmente distribuída de servidores proxy empregados em muitos data centers. O objetivo de uma CDN é fornecer conteúdo aos usuários finais com alta disponibilidade e alto desempenho. CDNs fornecem uma grande parcela do conteúdo atual da Internet, incluindo objetos web (texto, gráficos e scripts), objetos para download (arquivos de mídia, software, documentos), aplicativos (e-commerce, portais), streaming de mídia ao vivo, mídia de streaming on-demand e redes sociais. (https://en.wikipedia.org/wiki/Content_delivery_network)

Conteúdo No contexto deste documento, utilizamos "conteúdo" no sentido geral para descrever informações encontradas na Internet. Este conteúdo pode ser um documento completo ou apenas um parágrafo de um texto, imagem, vídeo, ou até mesmo apenas áudio (como um podcast). O conteúdo pode estar em páginas da web visualizadas em um navegador ou pode ser acessado por meio de ferramentas mais especializadas, como um aplicativo personalizado.

DNS O Sistema de Nomes de Domínio (DNS) é um sistema hierárquico descentralizado de nomenclatura para computadores, serviços ou outros recursos conectados à Internet ou a uma rede privada. Ele associa várias informações a nomes de domínio atribuídos a cada uma das entidades participantes. O mais importante é que ele converte de modo mais imediato os nomes de domínio memorizados em endereços IP numéricos, necessários para a localização e identificação de serviços de computadores e dispositivos com os protocolos de rede subjacentes. Ao fornecer um serviço de diretório mundial e distribuído, o Sistema de Nomes de Domínios é um componente essencial da funcionalidade da Internet, em uso desde 1985. (https://en.wikipedia.org/wiki/Domain_Name_System)

DPI A Inspeção Profunda de Pacotes (DPI) é uma forma de filtragem de pacotes de rede que examina a parte de dados (e possivelmente também o cabeçalho) de um pacote, enquanto este passa pelo ponto de inspeção, buscando falta de conformidade do protocolo, vírus, spam, invasões ou critérios definidos para decidir se o pacote pode passar ou se precisa ser tratado de outra forma, incluindo seu descarte. (https://en.wikipedia.org/wiki/Deep_packet_inspection)

Ilegal No contexto deste documento, utilizamos "ilegal" para descrever o conteúdo proibido em um contexto nacional, independente do motivo para tal proibição. O conteúdo pode ser ilegal porque viola um direito autoral (ou outro tipo de propriedade intelectual), como um filme pirateado. O conteúdo pode ser ilegal porque é censurável por razões morais, como obscenidade ou pornografia infantil. Pode ser conteúdo ilegal porque as autoridades nacionais desejam suprimi-lo ou o consideram ofensivo, como um desenho representando o Presidente de um país de forma adversa. O conteúdo ilegal em uma jurisdição pode ser completamente legal em outra. O conteúdo ilegal em um contexto (como uma comédia indecente, se vista por crianças) pode ser completamente legal em outro (se assistida por adultos), mesmo dentro da mesma jurisdição.

Endereço IP Um endereço IP (abreviação de endereço de protocolo Internet) é um identificador atribuído a cada computador e outros dispositivos (p.ex., impressora, roteador, dispositivo móvel, etc.) conectados à Internet. Ele é usado para localizar e identificar o nó em comunicações com outros nós da rede. (https://en.wikipedia.org/wiki/IP_address)

Falso negativo Um falso negativo ocorre quando o conteúdo não é bloqueado, mas deveria ter sido. Por exemplo, se farmácias ilegais estão sendo bloqueadas, uma farmácia ilegal recém-criada poderá não ser bloqueada, se o servidor ainda não tiver sido adicionado à lista de bloqueios. Isso seria chamado de falso negativo.

Falso positivo Um falso positivo ocorre quando algum conteúdo é bloqueado, mas não deveria ter sido. Por exemplo, se conteúdo pornográfico estiver sendo bloqueado, informações culinárias sobre peito de frango poderão ser bloqueadas, se o bloqueio tiver usado uma pesquisa de palavras-chave mal elaborada. Isso seria considerado um falso positivo.

TLS/SSL Protocolo Transport Layer Security (TLS) e seu predecessor, Secure Sockets Layer (SSL), frequentemente chamados em conjunto de "SSL", são protocolos de criptografia que fornecem segurança nas comunicações em uma rede de computadores. Diversas versões dos protocolos têm amplo uso em aplicações como navegação na web, e-mail, fax pela Internet, mensagens instantâneas e Voice-over-IP (VoIP). Os sites utilizam o protocolo Transport Layer Security (TLS) para proteger todas as comunicações entre os servidores e navegadores. O TLS tem como principal objetivo fornecer privacidade e integridade de dados entre duas aplicações de computador que estejam se comunicando.
(https://en.wikipedia.org/wiki/Transport_Layer_Security)

URL Uniform Resource Locator (URL), geralmente chamado de endereço web, é uma referência a um recurso da web que especifica sua localização na rede e um mecanismo para a sua recuperação. URLs ocorrem com maior frequência para referência a páginas da web (https), mas também são usados para transferência de arquivos (ftp), e-mail (mailto), acesso a bancos de dados (JDBC) e muitas outras aplicações. A maioria dos navegadores exibe um URL de uma página da web acima da página em uma barra de endereços. Um URL típico poderia ter a forma https://www.exemplo.com/index.html, que indica um protocolo (https), um hostname (www.exemplo.com) e um nome de arquivo (index. html).
(https://en.wikipedia.org/wiki/Uniform_Resource_Locator)

VPN A Virtual Private Network (VPN) estende uma rede privada entre uma rede pública, como a Internet. Ela permite que os usuários enviem e recebam dados entre redes compartilhadas ou públicas, como se os dispositivos de computação deles estivessem conectados diretamente à rede privada. Portanto, aplicativos em execução através da VPN, podem beneficiar a funcionalidade, a segurança e o gerenciamento da rede privada.
(https://en.wikipedia.org/wiki/Virtual_private_network)

Para leituras adicionais

As publicações a seguir podem interessar aos leitores em busca de informações adicionais sobre este tópico.

Documentos técnicos da Força-Tarefa de Engenharia da Internet

"A Survey of Worldwide Censorship Techniques" (Uma pesquisa sobre técnicas mundiais de censura) (Esboço da IETF draft-hall-censorship-tech-04) https://tools.ietf.org/html/draft-hall-censorship-tech-04

"Technical Considerations for Internet Service Blocking and Filtering" (Considerações técnicas para bloqueio e filtragem de serviços de Internet) (RFC 7754) https://tools.ietf.org/html/rfc7754

Documentos de políticas, pesquisas e históricos

"Filtering, blocking and take-down of illegal content on the Internet" (Filtragem, bloqueio e remoção de conteúdo ilegal na Internet), Conselho Europeu, 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" (Liberdade de expressão sem filtros: como o bloqueio e a filtragem afetam a liberdade de expressão), Artigo 19, 2016.
https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

"Freedom on the Net 2016" (Liberdade na net 2016), Freedom House, novembro de 2016.
https://freedomhouse.org/report/freedom-net/freedom-net-2016

"Internet Society Perspectives on Domain Name System (DNS) Filtering" (Perspectivas da Internet Society sobre o Sistema de Nomes de Domínios), Internet Society, 2012.
https://www.Internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf

"Network Neutrality" (Neutralidade na rede), 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 Respostas Políticas à Violação de Direitos de Propriedade On-Line), Internet Society, 2011.
https://www.Internetsociety.org/sites/default/files/bp-copyrightpolicy-20110220-en-1.pdf

Agradecimentos

A Internet Society agradece penhoradamente o auxílio de Joel Snyder, da Opus One, na preparação deste documento.

O relatório foi supervisionado por Nicolas Seidler e Andrei Robachevsky, da Internet Society.

O documento contou com revisões, comentários e apoio de diversos membros da equipe da 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 à equipe de Comunicações da Internet Society pela criação do aspecto visual deste documento e pela promoção de seu lançamento: James Wood, Beth Gombala, Lia Kiessling, Allesandra Desantillana.

Por fim, mas não menos importante, o documento foi significativamente aprimorado, graças à colaboração de diversos membros de divisões da Internet Society, por membros da organização e membros individuais, assim como pelo Conselho de Conselho Fiscal atual e anterior da Internet Society.

Internetsociety.org

Galerie Jean-Malbuisson 15,
CH–1204 Genebra, Suíça
Fone +41 22 807 1444

1775 Wiehle Avenue, Suite 201
Reston, Virgínia 20190, EUA
Fone +1 703 439 2120