SAC127: DNS Blocking Revisited

ISPCP Webinar: Implementing DNS Blocking Responsibly
13 May 2026

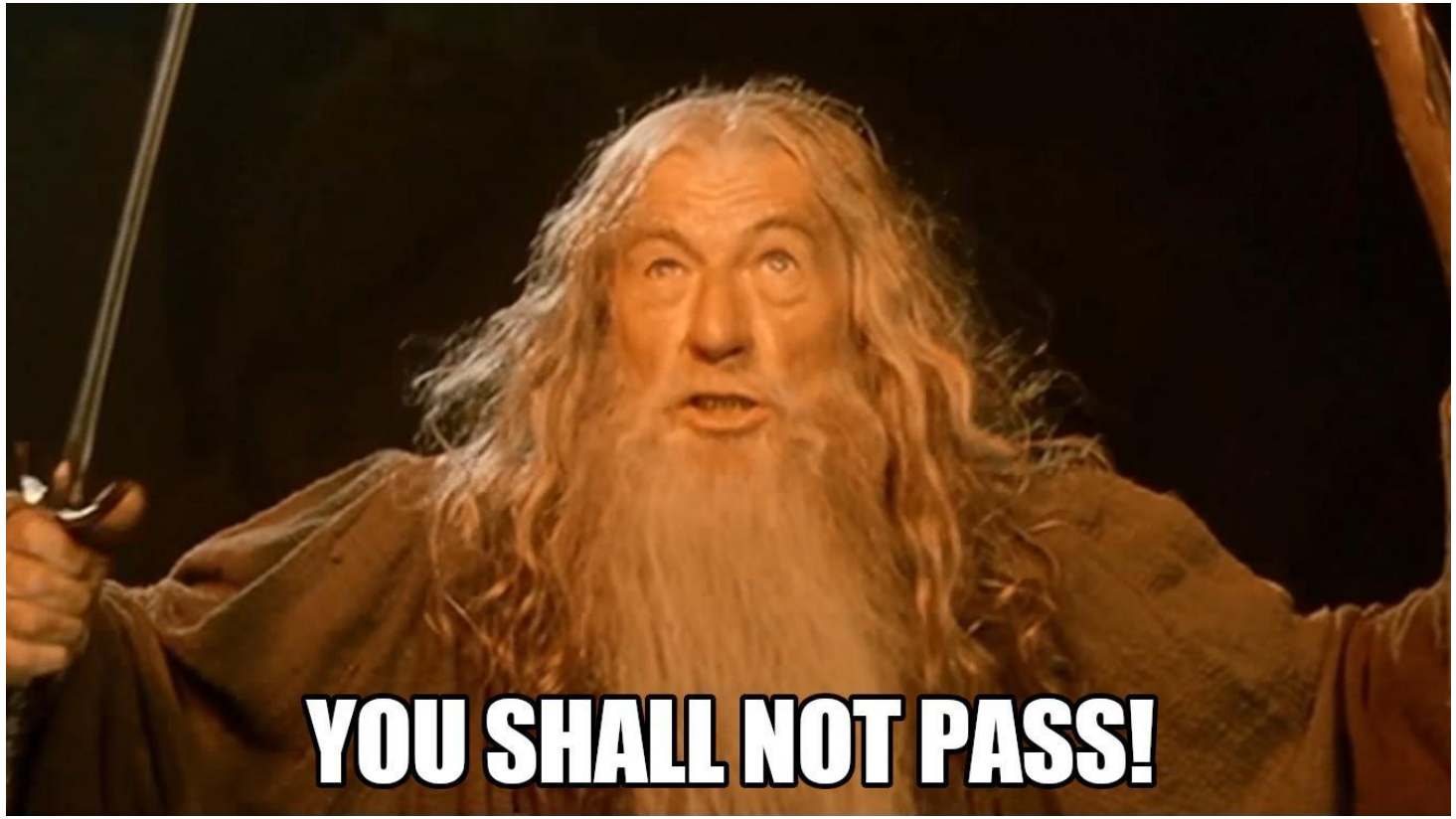
Greg Aaron

SAC127: DNS Blocking Revisited

- This report focuses on the technical means by which DNS blocking can be accomplished, and the effects—both intended and unintended—of its use in different contexts.
- Purpose is to advise the Internet community – especially policy-makers and government officials – of the implications & consequences of using DNS blocking

What is DNS Blocking?

- DNS blocking is a technique that restricts access to domain names
- **Goal**: Prevent a set of users from accessing content and services that use a domain name.
- Accomplished by either blocking DNS queries or directing user to a different destination.
- Blocking affects all services that use DNS lookups, including Web, email, network management.

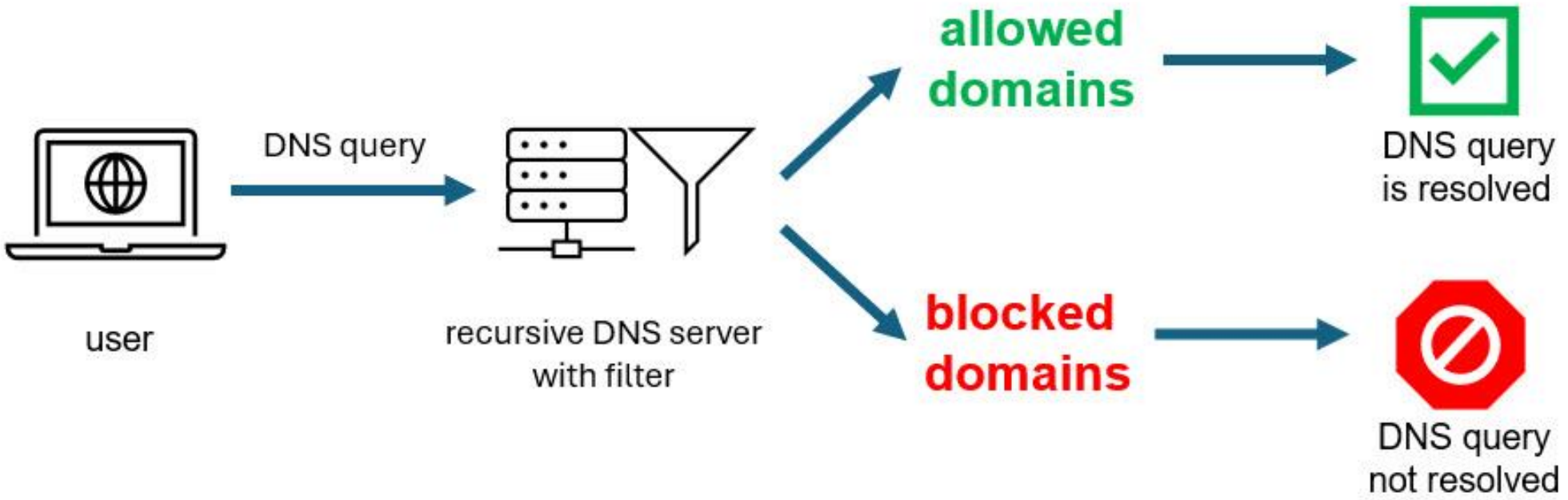

YOU SHALL NOT PASS!

What is DNS Blocking?

- DNS blocking is a *tool*. Like any tool, it can be used for different purposes, and with different motivations.
- Does **not** remove the content or service from the Internet.
- A more limited alternative to suspending a domain name (which makes the domain not work at all).
- Can be wielded with varying degrees of effectiveness and precision.
- There are ways to circumvent DNS blocking.
- DNS blocking can have serious and unintended side-effects.

Blocking Methods

Methods for DNS Blocking



1. **Query Response Does Not Provide Resolution**: Recursive resolver *tells the user that a resolving domain does not exist.* Modifies the authoritative server response.

Domain Blocking at a Recursive Resolver

2. Via Redirection: *Points the user to another domain.* Recursive resolver modifies the authoritative server response, returning an IP address other than the IP address of the blocked domain. (This could redirect to a message indicating the site is being blocked.)

3. Via Query Non-Response: Recursive resolver *ignores queries* for a requested domain (end user may interpret to mean that the resolver is unusable).

DNS blocking can be effective if the user relies on the DNS infrastructure where the blocking is implemented.

Domain Suspension, Domain Seizure

- Suspension is not “DNS blocking” but achieves a similar goal: prevents access to a domain and its content.
- Registrar or registry operator can suspend a domain.
- Removes domain from the DNS zone. Domain stops resolving for everyone.
- Domains can also be “seized”: domain taken away from control of the old registrant. The domain may redirect to different content.

Motivations and Examples

Motivation: For Security Purposes

Network operators/services block access to domains posing security risks to users

- A DNS blocklist is a list of domain names considered dangerous. (Phishing, malware, spam, etc.)
- The use of DNS blocking for security and anti-abuse purposes is pervasive, and most Internet users and organizations are protected via DNS blocking.
- All major email providers, some public DNS resolvers, and major web browsers use DNS blocklists.

Motivation: Content Access within an Organization

Organizations use DNS blocking to shield/block users on their networks from content and services determined by the organization to be inappropriate.

- Organizations (companies, schools, libraries, government offices) commonly restrict content/services on their networks/devices.
- Caregivers restrict minors in the home from accessing content deemed inappropriate
  - Examples: gambling, pornography
- The network operator has rules for use of its network.

Motivation: Legal and Political Reasons

Government authorities/courts block content deemed illegal or harmful.

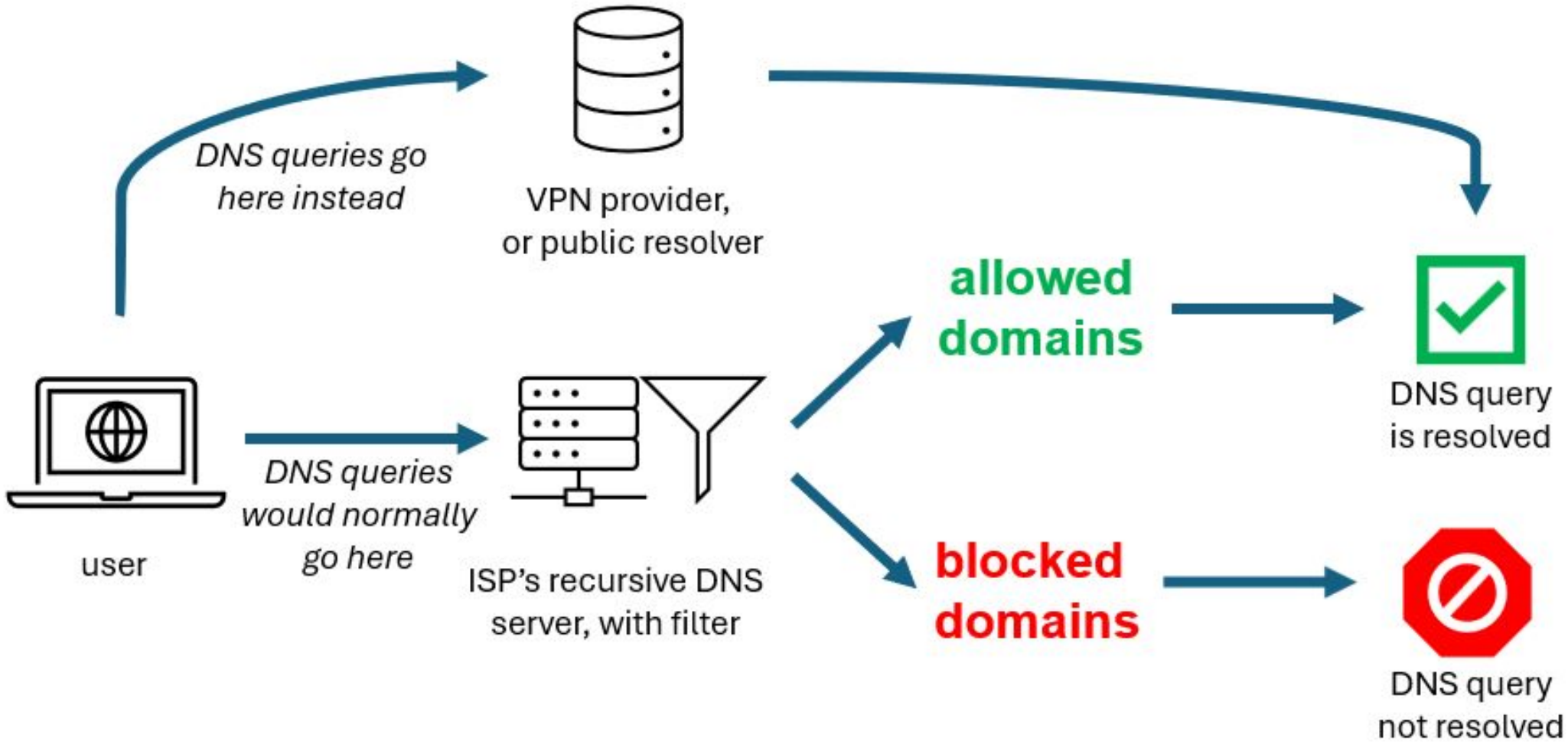
- The controversial content may be hosted outside the jurisdiction.
- A government may have no legal right or ability or desire to take the material off the Internet. The government may therefore focus on preventing access to the material from within its jurisdiction. DNS blocking can provide a means to accomplish that goal.
- Censorship: limiting access to information deemed subversive or politically destabilizing
- See case studies in the paper.

A Note

"The SSAC notes that whether an action constitutes censorship, or the legality of any specific case of DNS blocking, will depend upon local laws (which vary widely across the globe), and can involve personal convictions, about which people may vary in good faith. For these reasons, the SSAC does not make statements in this report about the propriety of specific cases of DNS blocking – such discussions are more suited for political fora. The merits or advisability of governmental or other attempts to control access to resources on the Internet are beyond the scope of this report."

Circumventing DNS Blocking

Circumvention: Go around the blocking

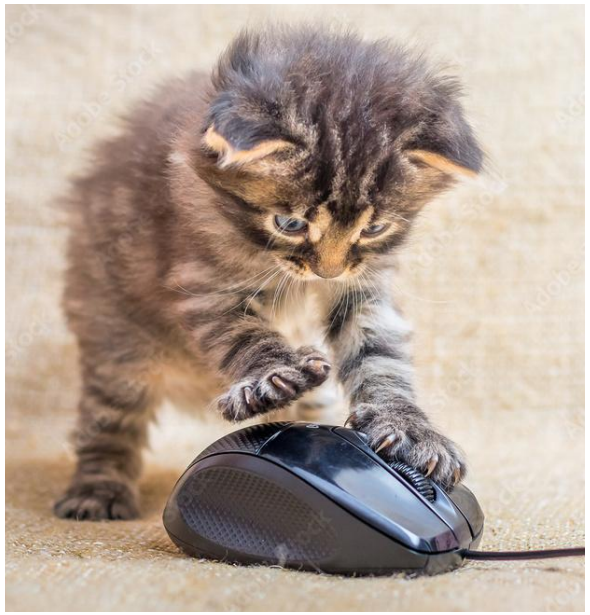


Circumvention by users: Alternative DNS Servers

- User changes DNS settings on their device, to use a resolver that doesn't enforce the same blocking restrictions.
- Public resolvers: offer reliability, security, lack of filtering.
  - Easy to implement, especially for non-technical users. ~21% of users worldwide use public resolvers.
  - Examples:
    - Google Public DNS (8.8.8.8)
    - Cloudflare's public resolver (1.1.1.1)
    - Quad9 (9.9.9.9)
- Government-sponsored resolvers such as DNS4EU

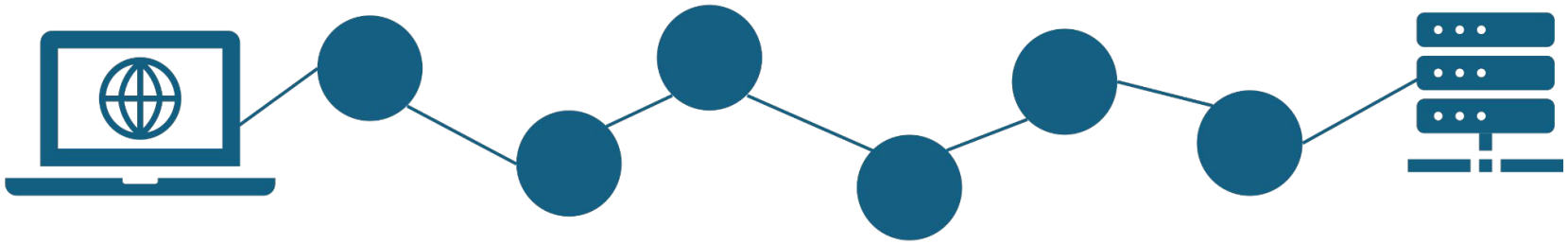
Circumvention by users: VPNs (Virtual Private Networks)

- Encrypt Internet traffic and route through alternative servers. Allows users to:
  - Bypass geographical restrictions (example: streaming)
  - Evade censorship
  - Enhance privacy and anonymization
  - Secure DNS resolution
- Use of VPNs is widespread
- Ongoing “cat and mouse” game



Circumvention by users: Anonymization and Obfuscation Tools

- Similar to VPN, but routes encrypted Internet traffic across multiple **nodes** rather than **end-to-end** – this significantly enhances anonymity



- Examples include Tor (“The Onion Router”) and Psiphon
- Some network operators and governments block access to Tor

DNSSEC Validation

- DNSSEC can detect “spoofing” – responses as a result of DNS blocking
- DNSSEC validation protects clients by minimizing spoofed responses.
- Technically capable users may configure other resolvers to obtain the blocked response.

Circumvention: Lessons

- The effectiveness or “success” of DNS blocking is often a matter of degree.
- DNS blocking may predominantly affect users who are less technically savvy and are not aware of circumvention methods.
- DNS blocking may motivate content or service providers to work around blocking.
- Internet Service Providers (ISPs) & network operators will not be able to use DNS blocking to completely prevent access to a given piece of content, domain, or service.

Evolutionary Changes & Trends

Encrypted DNS: DoH, TLS, and DoQ (Collectively, DoX)

- Innovations of various encryption mechanisms designed to safeguard DNS queries & responses
  - DNS over Transport Layer Security (TLS)
  - DNS over HTTPS (DoH)
  - DNS over Dedicated QUIC Connections
- Enhance user privacy and security by encrypting DNS traffic, between client/resolver & recursive/authoritative resolvers

Extended DNS Error

- Traditionally, DNS errors provide users with little information about the reasons behind failed resolutions.

- RFC8914: Extended DNS Errors enable resolvers to provide more informative error codes & communicate the nature of the DNS blocking
  - For example: “Extended DNS Error Code 16 - Censored”

DNS Blocking: Considerations and Consequences

Over-Blocking

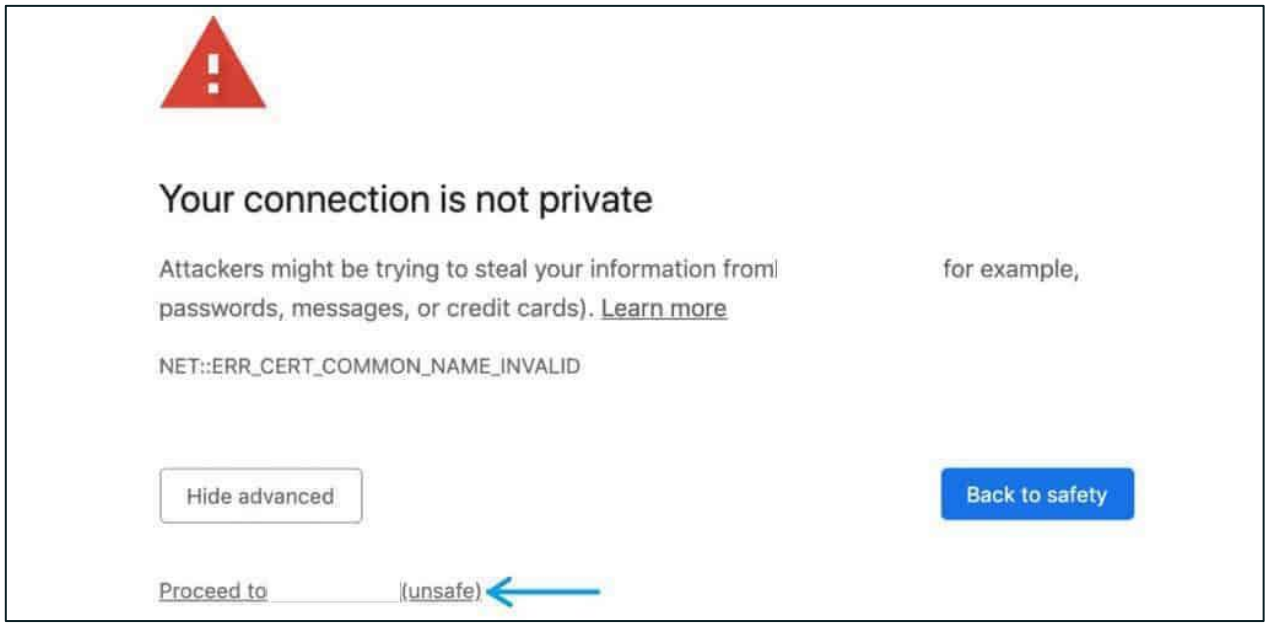
- Blocking at the wrong level
  - If the party blocks **.TLD**, it will block all domains in the TLD, which may include many more services and content than intended.
  - If the party blocks **example.TLD**, it blocks everything at and beneath that domain, such as **third-level.example.TLD**
- Blocking a domain by accident.

Collateral Damage

- DNS blocking can be geographically imprecise. May affect users across borders, in other jurisdictions.
- Blocking may affect domains that provide services for other domains, causing collateral damage beyond the intended scope of the block.
- See case studies in the paper.

Trains Users to Disable or Ignore Security Controls

- DNS blocking through redirection may trigger warnings as a result of Transport Layer Security (TLS) errors for websites
- Users may ignore these warnings on interstitial pages in browsers
- This trains users to ignore name mismatch certificate errors



Disclosure and Transparency

- Does a party agree to blocking? Do they know blocking is taking place?
  - Within organizations, blocking may be a condition.
  - Organizations choose their providers.
- It may be impractical to disclose DNS blocking policies or to transparently share a list of domains being blocked.
- DNS blocking can be misdiagnosed as a hosting outage, a misconfiguration, or a malicious attack.
- End users, network administrators, service providers, and other parties may make mistaken attempts to mitigate the problem.

SSAC Recommendations

SAC127 Recommendations

Recommendation 1: SSAC recommends that any entity implementing or mandating DNS blocking understand the implications of the technology.

SAC127 Recommendations

Recommendation 2: SSAC recommends that DNS blocking implemented by any entity—by a government or any organization that has policy, legal, or operational control over a network or service—follow these guidelines:

A. The entity should determine whether DNS blocking will fulfill its objectives.

B. The entity should have a clear policy about what and how it will block, with well-defined review and decision-making processes that minimize risk.

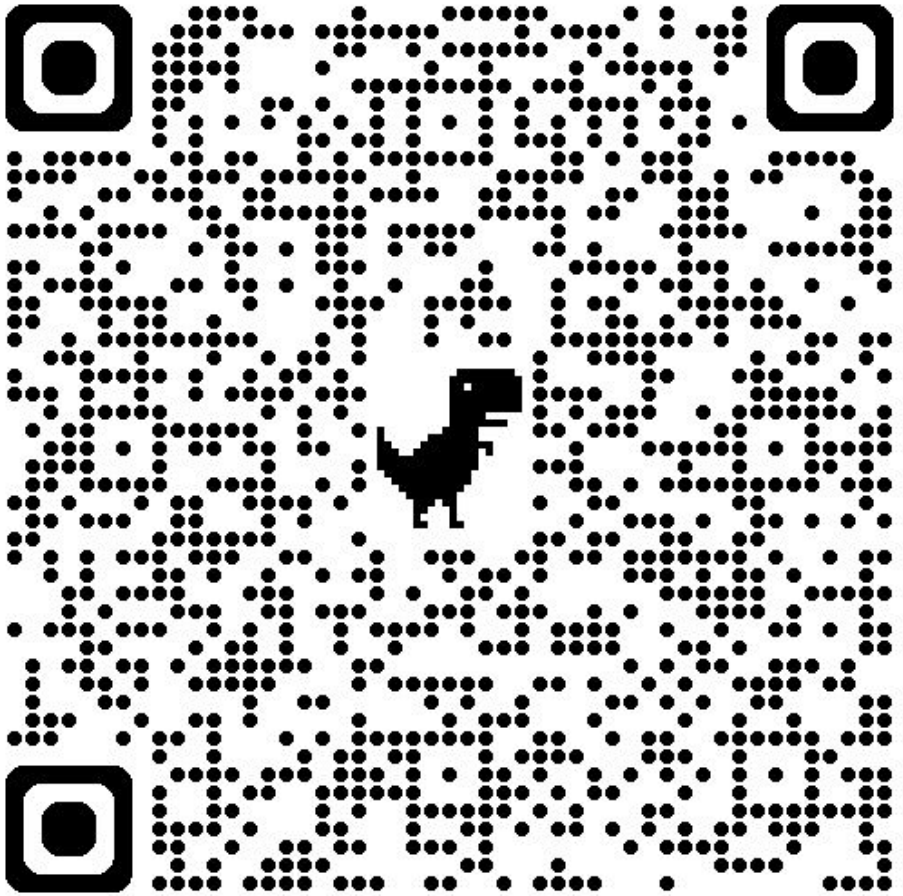
C. The entity should implement the policy using a technique that minimizes overblocking or collateral damage that could affect its users.

D. The entity should not affect networks or users outside its administrative control.

Recommendation 3: SSAC recommends that operators of recursive servers use RFC8914 DNS Extended Error codes (see section 6.6 Extended DNS Error) to indicate to end users and troubleshooters that DNS blocking is taking place.

SAC127: DNS Blocking Revisited

Visit bit.ly/4kw1X3R or scan the QR code for **SAC127: DNS Blocking Revisited**



Have additional questions?

Email us at ssac-staff@icann.org