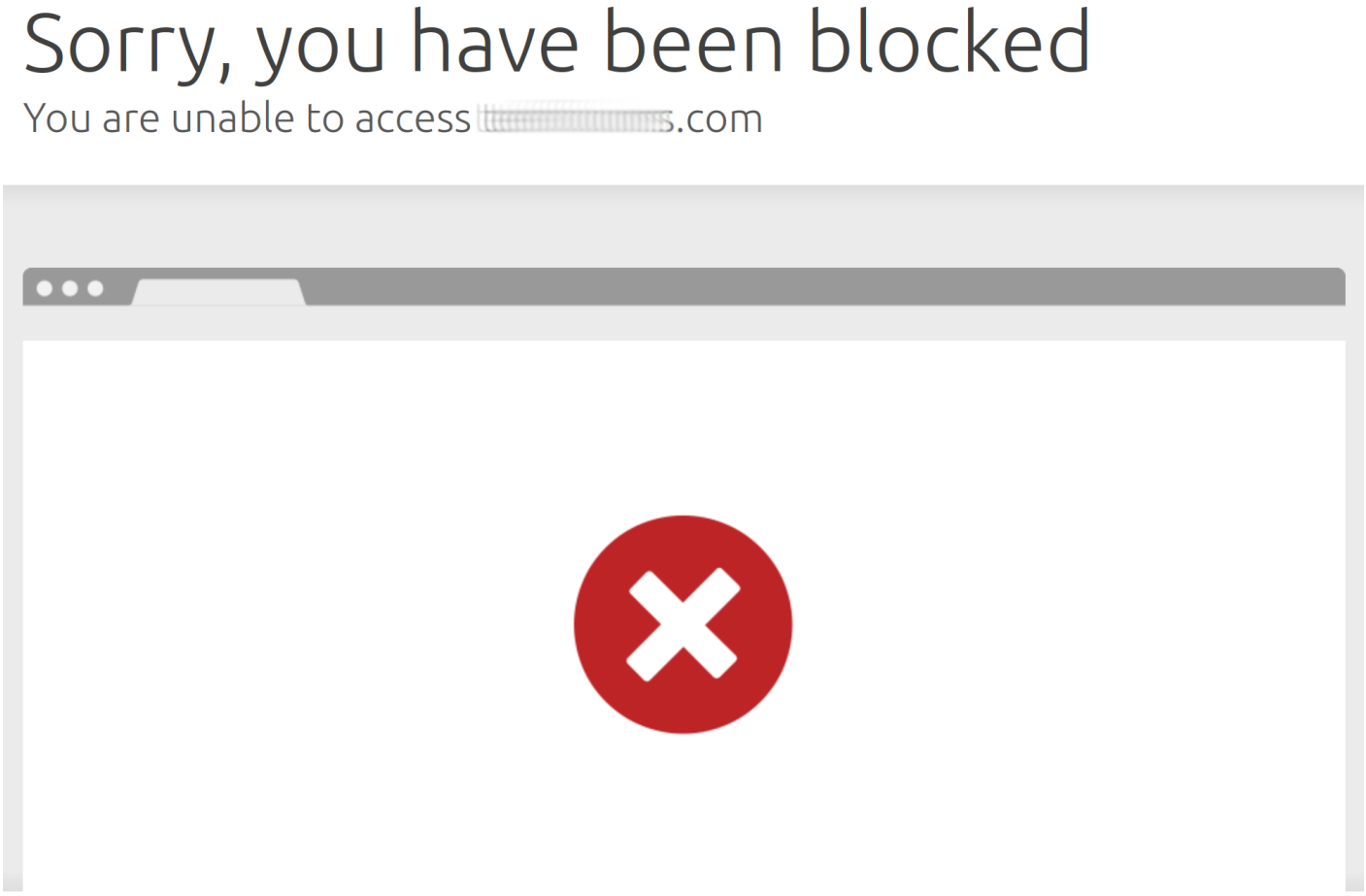
Resolve Cloudflare Block Pages

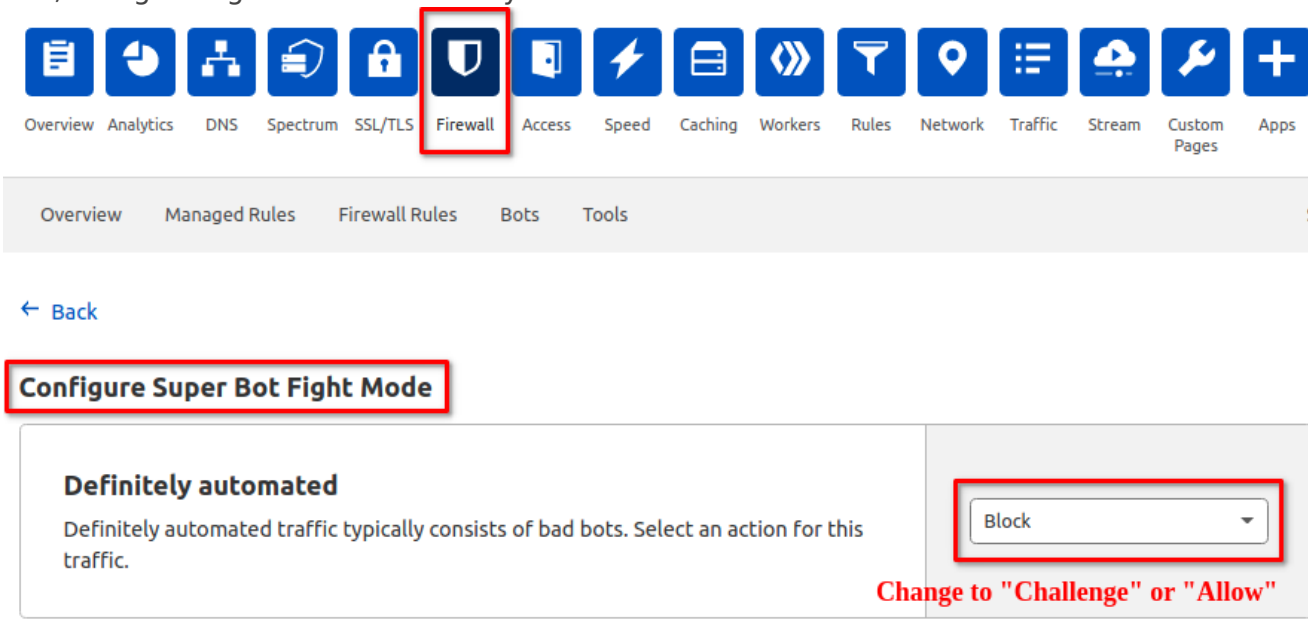
Problem

You're running into a block page from Cloudflare that indicates you've been blocked. No options are given to complete a CAPTCHA or otherwise proceed.



Solution

1. Take note of the Ray ID on the Cloudflare block page.
2. Send your access complaint, along with the Ray ID, to the support/administration team for the website that you're encountering the problem on. They can use this information to locate the Cloudflare firewall rule that's causing the false positive block event.[1]
   If a specific firewall rule can't be found, generally adjusting the Bot handling settings will resolve the problem:
   - Under **Firewall**, select **Bots**, then **Configure Super Bot Fight Mode**.
   - In the **Configure Super Bot Fight Mode**, change the setting on *Definitely automated* from "Block" to "Challenge".
     This will present all suspected *definitely automated* bot activity with a Cloudflare challenge/CAPTCHA page, which will both allow the website admins to protect their site, and give legitimate users a way of recourse.



3. Furthermore, we strongly recommend you ask the website administrators raise a support ticket with Cloudflare, including the Ray IDs you noted, so Cloudflare can improve their automated traffic classifications system. **This is the only way that a long-term solution will be achieved.**

[1]Web administrators using Cloudflare may find this third-party blog post helpful in troubleshooting: Finding a Cloudflare event by Ray ID.

Explanation

Short version

Cloudflare has software that analyses TLS (encryption) handshakes in an attempt to determine whether inbound traffic to a website is originating with a human or a bot. Unfortunately, Cloudflare is incorrectly classifying DrawBridge-filtered traffic as a malicious bot.

Detailed version

The traffic to/from all HTTPS websites travels over one or more encrypted sessions, negotiated between the browser and the destination web server. Only the web server and the browser can read the content -- the traffic is scrambled to anyone else who may see the session(s), including any transit/internet-service-provider equipment, because they don't have the secret keys that secure the session.

This is problematic when it comes to web content filtering: once a session is established with "amazon.com", for example, nothing else can be known about that session to anyone else. If you're a parent or business network administrator, you may care very much what happens on your network, but don't have visibility into what is actually happening.

Enter the DrawBridge: When a web request is made, the DrawBridge steps in and presents itself as the webserver to the browser, and negotiates a secure session. Then the DrawBridge itself negotiates another, separate, secure session to the destination webserver.

And this is where the issue lies: Cloudflare sees the TLS handshake initiated by the DrawBridge (rather than the browser) and incorrectly classifies the handshake as one of a malicious bot.

Note: the DrawBridge does not generally perform TLS inspection on banking/financial websites. If you've indentified a case of this, please send a detailed email to support@compassfoundation.io.

Further Reading

Link: FAQ: Is TLS inspection "bad" or "breaking encryption" or "weakening security"?

Link: What is TLS fingerprinting?

Alternate workaround

In the event no resolution can be arranged with the administrators of the Cloudflare firewall settings for the website, an alternate workaround is available: Add the domain of the site in focus to the **Bypass Filter** policy in the DrawBridge Access Policy Dashboard, and apply the changes.

It may be nessesary to close and re-open your browser to ensure that a new secure session gets established.

Note that this **disables DrawBridge filtering and reporting on all of that domain**.

Revision #8
Created 11 January 2023 15:43:26 by Marvin M.
Updated 13 February 2024 13:55:29 by Marvin M.