Using CDN for Entire Website and Country Blocking - Part 1

Posted At : November 29, 2018 7:59 AM | Posted By : Wil Genovese
Related Categories: ColdFusion, Coldfusion Security, Hosting and Networking, Security, AWS

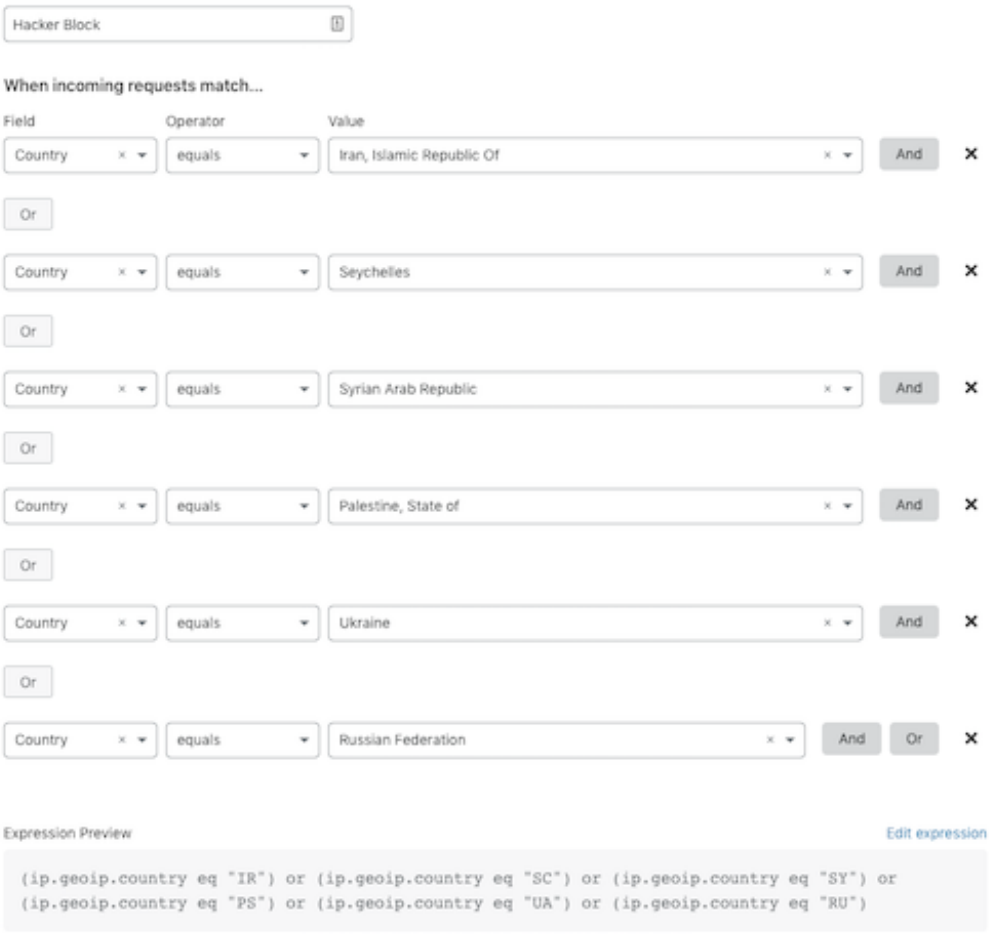
CF Webtools has been asked numerous times to block an entire country or countries by many clients. The issue is that there's a lot of hacker activity from certain identified countries and the client(s) does not do any business with those countries. Typically it's entire server hacking attempts, but more recently it's to use the client's shopping cart to "test" stolen credit cards. This is a very serious problem and as such clients are asking us to help them prevent this from happening. One potential solution is to block the IP addresses that these attacks are coming from. I refer to this as the Whack-A-Mole method because it's just like that arcade game. As soon as you block one IP they switch to another IP address.

We need a better solution. I looked into what we could do and how reasonable and feasible the various options are in terms of technology and cost. In this article I'm writing about using CloudFlare CDN to block entire countries.

CloudFlare
I was not familiar with CloudFlare other than it's a CDN. They do offer advanced services for a price. There is a free tier that has CDN capability and limited Firewall features. The firewall features include the ability to setup 5 firewall rules.

To test the features and capabilities of CloudFlare I created a free account for myself and setup my blog to use CloudFlare. My blogs uptime is not critical like the client's business is and it gets real traffic thus it can be used to test various features.

Using the free firewall features I can block multiple countries in a single firewall rule. The rules allow for chaining filters with AND OR statements. See the example below.



I don't know yet if there is a limit to the number of conditions I can add to a single rule. However, at the moment it seems to be sufficient.

The negative side effect that I can see so far is that all the IP addresses that get logged on the origin web server are from CloudFlare. This defeats many clients needs/desires to have a valid IP address of their valid customers. Cloudflare does offer the option to pass through the original HTTP headers, but that is under their top Enterprise plan. They do not provide a cost for this. You need to request an estimate.

CloudFlare does pass through custom headers that has the original IP and other custom headers. However, these are not standard and web servers need to be configured to first read the custom header fields and then the application code needs to be updated to use the custom headers fields. It's far easier to do this in Apache than it is in IIS. IIS does not allow this to be done at a global level meaning each IIS site must be configured for the custom headers. Additionally, you may need to custom code the web application to read X-Forwarded-For no matter which web server you are using.

Another issue is that CloudFlare requires you move your DNS to them. Depending on the client, gaining access to their DNS and registrar can be challenging.

Part 2 will cover using AWS CloudFront to achieve the same results.

cfwebtools.com.