



Securing Your Organization from DDoS Attacks

In today's digital landscape, the internet serves as a bustling marketplace, a vital bridge for communication, and a crucial lifeline for countless businesses. Yet, lurking within this seemingly benign realm lies a dark shadow – the Distributed Denial-of-Service (DDoS) attack. Imagine a relentless bombardment of malicious traffic flooding your servers, overwhelming them like a digital tidal wave, bringing your online operations crashing down.

What is a DDoS Attack and How Does it Work?

Picture a massive, coordinated siege on your online castle. Instead of swords and catapults, the attackers wield an army of bots, infected devices, and compromised servers. These bots, controlled by malicious actors, unleash a torrent of requests aimed at your servers, overwhelming them with legitimate-looking traffic. Imagine an online store bombarded with millions of simultaneous login attempts – servers buckle under the strain, legitimate users get locked out, and your operations come grinding to a halt. That's the crippling effect of a DDoS attack.

Motives and Tactics:

So, why do attackers unleash these digital sieges? The reasons are as varied as the attackers themselves. Some aim to extort businesses, demanding ransom in exchange for ceasing the attack. Others seek to silence dissent, crippling websites that host opposing viewpoints. Still others engage in cyber vandalism, relishing the chaos they inflict.

The Lab: Building Your Wall of Defence

Now, let's get practical. How can you fortify your online fortress against these digital onslaughts? Here's your DDoS mitigation lab, complete with a Cloudflare WAF rule to counter a specific attack type:

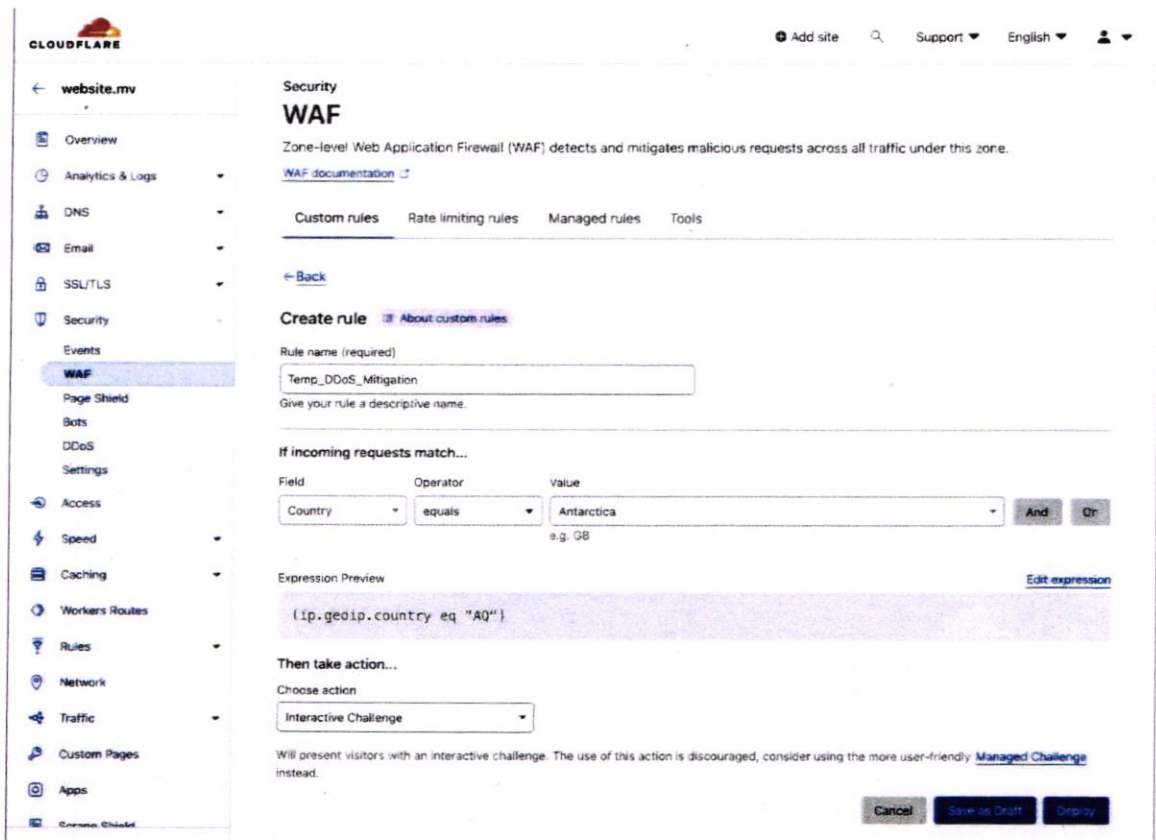
Target: Geolocation-based attacks exploiting vulnerable regions.

Weapon: Cloudflare WAF rule with Browser Integrity Check and Interactive Captcha.

Step 1: Identify the Geolocation:

Analyse your traffic logs and identify regions with unusually high traffic volumes or suspicious activity patterns. For example, a sudden surge in traffic from Antarctica might raise red flags.

Step 2: Create the WAF Rule:



The screenshot shows the Cloudflare WAF dashboard for a site named 'website.mv'. The left sidebar contains navigation options like Overview, Analytics & Logs, DNS, Email, SSL/TLS, Security, Events, WAF, Page Shield, Bots, DDoS, Settings, Access, Speed, Caching, Workers Routes, Rules, Network, Traffic, Custom Pages, and Apps. The main content area is titled 'Security WAF' and includes a description: 'Zone-level Web Application Firewall (WAF) detects and mitigates malicious requests across all traffic under this zone.' Below this, there are tabs for 'Custom rules', 'Rate limiting rules', 'Managed rules', and 'Tools'. The 'Create rule' section is active, showing a rule named 'Temp_DDoS_Mitigation'. The configuration is as follows:

Field	Operator	Value
Country	equals	Antarctica

The expression preview shows: `(ip.geoip.country eq "AQ")`. Under 'Then take action...', the chosen action is 'Interactive Challenge'. A note states: 'Will present visitors with an interactive challenge. The use of this action is discouraged, consider using the more user-friendly [Managed Challenge](#) instead.'

- Navigate to the Cloudflare WAF dashboard.
- Click "Create Rule".
- Set the "Field" to Country and input the value of the country where you suspect the attacks are originating from.
- Under "Action," choose "Interactive Challenge."

Step 3: Monitor and Refine:

- Keep an eye on your WAF dashboard and traffic logs for effectiveness.
- Fine-tune the rule parameters if needed to balance security with legitimate traffic flow.
- Remember, vigilance is key! Periodically review your WAF rules and overall security posture to adapt to evolving threats.
- Remember, for these steps to be effective, restrict access to your web servers to only trusted Cloudflare IP addresses. This minimizes attack surfaces and boosts DDoS protection. Monitor for potential false positives and update the whitelist with Cloudflare's latest IPs. Remember, even a small gate can secure a mighty fortress.

Cloudflare publishes a continuously updated list of IP addresses used for routing traffic (available at: <https://www.cloudflare.com/en-gb/ips/>). Download this list and implement firewall rules on your web server to allow access only from these IP addresses. This effectively acts as a whitelist, ensuring that requests only originate from Cloudflare's trusted network, significantly reducing the attack surface for DDoS assaults.

By understanding the nature of DDoS attacks and implementing strategic measures like the Cloudflare WAF rule, you can build a resilient online fortress. Remember, proactive defence is paramount in the digital age. So, arm yourselves with knowledge, fortify your infrastructure, and stand firm against the tide of DDoS attacks. Your online domain awaits!

Bonus Tips:

- Implement rate limiting on your web server to throttle excessive traffic.
- Utilize a Content Delivery Network (CDN) to distribute traffic and absorb attack waves.
- Partner with a DDoS mitigation service provider for advanced protection.
- Conduct regular security audits and vulnerability assessments.

Remember, staying vigilant and actively fortifying your defences is the key to maintaining a secure and resilient online presence in the face of ever-evolving cyber threats.

For specialized assistance or further guidance in enhancing your cybersecurity measures, don't hesitate to reach out to us at security@ncit.gov.mv.

