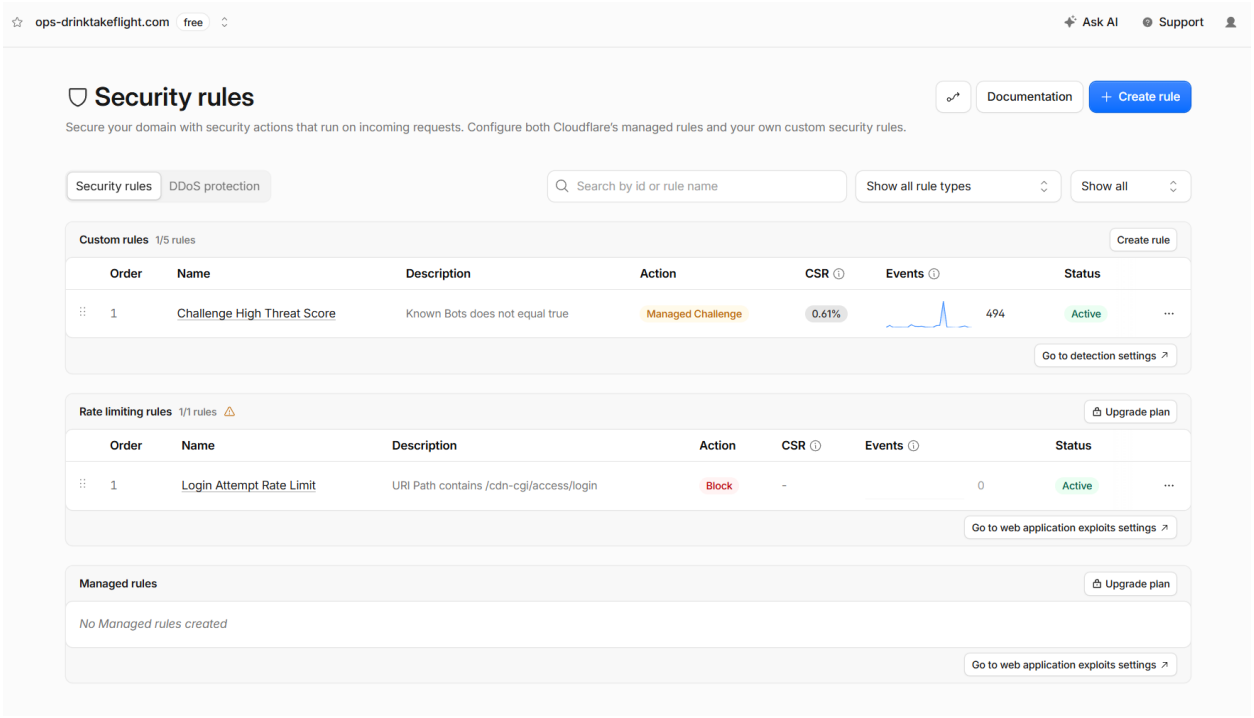

ops-drinktakeflight.com
free
Ask AI
Support
Security rules
Documentation
Create rule
Secure your domain with security actions that run on incoming requests. Configure both Cloudflare's managed rules and your own custom security rules.
Security rules
DDoS protection
Search by id or rule name
Show all rule types
Show all
Custom rules 1/5 rules
Create rule
Order
Name
Description
Action
CSR
Events
Status
1
Challenge High Threat Score
Known Bots does not equal true
Managed Challenge
0.61%
494
Active
Go to detection settings
Rate limiting rules 1/1 rules
Upgrade plan
Order
Name
Description
Action
CSR
Events
Status
1
Login Attempt Rate Limit
URI Path contains /cdn-cgi/access/login
Block
-
0
Active
Go to web application exploits settings
Managed rules
Upgrade plan
No Managed rules created
Go to web application exploits settings

Edit custom rule

Protect your website and API from malicious traffic with custom rules. Configure mitigation criteria and actions, or explore templates, for better security.

Rule name

Challenge High Threat Score

Give your rule a descriptive name.

When incoming requests match...

Field	Operator	Value
Known Bots	equals	

And Or

Expression Preview Edit expression

```
(not cf.client.bot)
```

19 / 4000 characters

Historical preview unavailable for field: Known Bots

Then take action...

Choose action

Managed Challenge

Presents an interactive or non-interactive challenge to the client

Execution order

Rules are evaluated sequentially in order. The position you choose determines at which point in this sequence your rule will evaluate the traffic.

Select order:

First

Status

Controls whether the rule actively evaluates incoming traffic

- Disabled
- Active

Save with API call

Edit rate limiting rule

Protect your website and API from malicious traffic with rate limiting rules. Configure mitigation criteria and actions for better security.

Rule name

Login Attempt Rate Limit

Give your rule a descriptive name.

When incoming requests match...

Field	Operator	Value
URI Path	contains	/cdn-cgi/access/login

And Or

e.g. /content

Expression Preview Edit expression

```
(http.request.uri.path contains "/cdn-cgi/access/login")
```

56 / 4000 characters

Total requests matched

0

0.0% of all traffic - Last 24 hours

With the same characteristics...

IP

When rate exceeds...

Requests	Period
3	10 seconds

Historical preview is only available for 1-minute, 5-minute, and 1-hour periods

Then take action...

Choose action

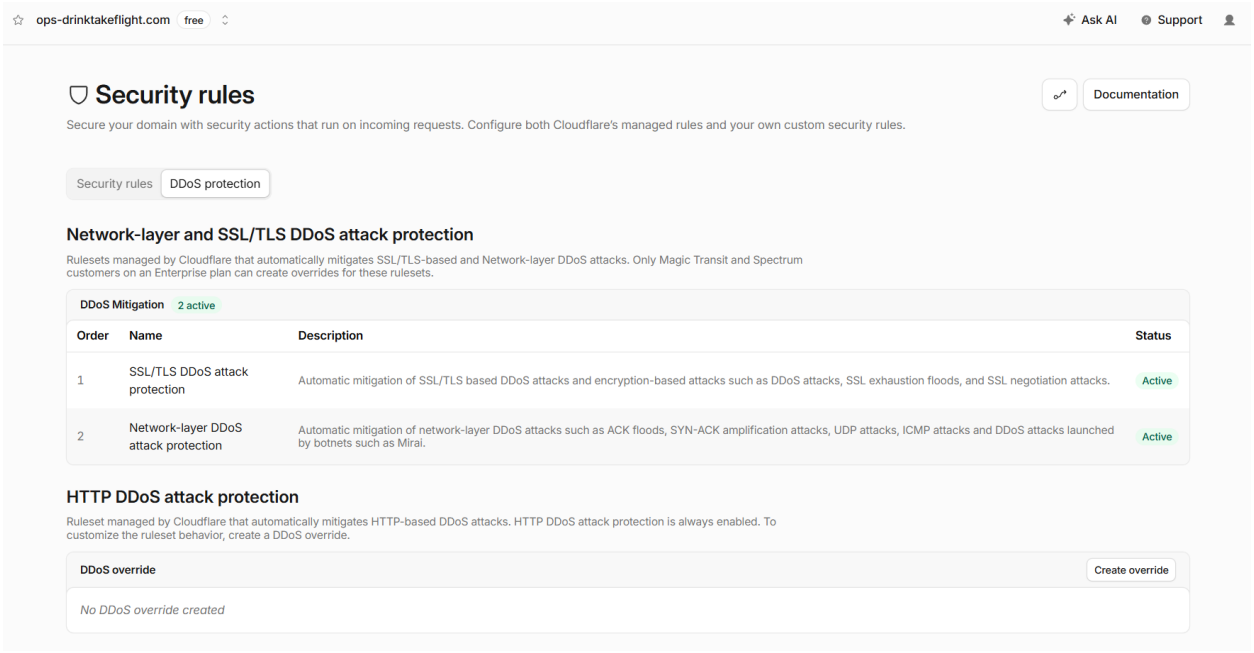
Block

Blocks matching requests and stops evaluating other rules

For duration...

Duration

10 seconds


ops-drinktakeflight.com
free
Ask AI
Support
Security rules
Documentation
Secure your domain with security actions that run on incoming requests. Configure both Cloudflare's managed rules and your own custom security rules.
Security rules
DDoS protection
Network-layer and SSL/TLS DDoS attack protection
Rulesets managed by Cloudflare that automatically mitigates SSL/TLS-based and Network-layer DDoS attacks. Only Magic Transit and Spectrum customers on an Enterprise plan can create overrides for these rulesets.
DDoS Mitigation
2 active
Order
Name
Description
Status
1
SSL/TLS DDoS attack protection
Automatic mitigation of SSL/TLS based DDoS attacks and encryption-based attacks such as DDoS attacks, SSL exhaustion floods, and SSL negotiation attacks.
Active
2
Network-layer DDoS attack protection
Automatic mitigation of network-layer DDoS attacks such as ACK floods, SYN-ACK amplification attacks, UDP attacks, ICMP attacks and DDoS attacks launched by botnets such as Mirai.
Active
HTTP DDoS attack protection
Ruleset managed by Cloudflare that automatically mitigates HTTP-based DDoS attacks. HTTP DDoS attack protection is always enabled. To customize the ruleset behavior, create a DDoS override.
DDoS override
Create override
No DDoS override created