

Forum:[Hack Forums](#)

Thread: [Rate Limit and Traffic Control](#)

Omniscient - October 12, 2016, 12:50 pm

We're now part of the beta for Cloudflare's "Traffic Control" feature.

It allows for rate limiting of individual pages with suspension of connection for a certain time.

Currently just index.php is limited to about 12 per minute. If you've load index more than that you're access is blocked to the entire domain for 15 minutes.

If you've loaded index 12 times within 1 minute that's excessive connecting and I'm not sure why you'd do that.

And this is a beta. Unsure how smart their triggers are and if they are correctly doing everything. It literally just started today and for all I know it's just HF that's in the early beta. Realistically we're all they need to test a feature like this.

And seriously, disable your userscripts if you run them and you're getting blocked. Userscripts behave in ways that will trigger this firewall.

If you're being blocked and you know for a fact you didn't hit the index.php 12 times within a minute you can PM me the RAY ID and your IP at the time in text form (NO SCREENSHOTS PLEASE). I can forward the data to Cloudflare for them to review.

ze-slade - October 12, 2016, 12:57 pm

Thanks for letting us know Omni, I don't why was I blocked earlier though? All I was doing was clicking "view new post", does that trigger it too somehow?

ra1d - October 12, 2016, 1:00 pm

This is a great feature, hopefully it is going to benefit the load on servers.

Omniscient - October 12, 2016, 1:17 pm

(Oct 12, 2016 12:57 PM)ze-slade Wrote: [\[CITE\]](#) Thanks for letting us know Omni, I don't why was I blocked earlier though? All I was doing was clicking "view new post", does that trigger it too somehow?

Sounds like earlier a lot of people were blocked. Could have been they didn't set the rule right. Again, this is a beta.

ze-slade - October 12, 2016, 1:18 pm

(Oct 12, 2016 01:17 PM)Omniscient Wrote: [\[CITE\]](#) Sounds like earlier a lot of people were blocked. Could have been they didn't set the rule right. Again, this is a beta.
Understandable, thanks for the response!

M?xim - October 12, 2016, 1:25 pm

Seems to be in great favor of the forum in general. Cheers and thanks.

Lante - October 12, 2016, 1:28 pm

I've heard people being blocked when visiting different pages, be it showthread.php, or search.php

(view new posts) or private.php (PMs). If this feature will eventually only look for index.php access violations then I am all in favor, as long as it won't damage other functions as it did today for a short period of time.

Granny Bacon - October 12, 2016, 1:30 pm

(Oct 12, 2016 01:28 PM)Lante Wrote: [\[CITE\]](#) I've heard people being blocked when visiting different pages, be it showthread.php, or search.php (view new posts) or private.php (PMs). If this feature will eventually only look for index.php access violations then I am all in favor, as long as it won't damage other functions as it did today for a short period of time.

It's still in beta, you gotta give it some time.

Lante - October 12, 2016, 1:32 pm

(Oct 12, 2016 01:30 PM)Granny Bacon Wrote: [\[CITE\]](#) It's still in beta, you gotta give it some time. Hence the usage of the word "eventually" ;)

Granny Bacon - October 12, 2016, 1:32 pm

(Oct 12, 2016 01:32 PM)Lante Wrote: [\[CITE\]](#) Hence the usage of the word "eventually" ;) Yup, I was reading too fast.. my bad.

Armada - October 12, 2016, 2:32 pm

Good to know, not sure why I would be loading the index so often so quickly however anyways. ?

That suggestion of the User scripts is great though. Thanks for letting us know.

Omniscient - October 12, 2016, 3:06 pm

(Oct 12, 2016 02:32 PM)Armada Wrote: [\[CITE\]](#) Good to know, not sure why I would be loading the index so often so quickly however anyways. ?

That suggestion of the User scripts is great though. Thanks for letting us know.

Attacks normally focus on a single attack vector. I'll be able to set rules for each page hopefully. Index page is often the target.

ze-slade - October 12, 2016, 3:10 pm

(Oct 12, 2016 03:06 PM)Omniscient Wrote: [\[CITE\]](#) Attacks normally focus on a single attack vector. I'll be able to set rules for each page hopefully. Index page is often the target.

If you do limit most pages, please don't limit the new pages really low. I always click on that at least 3 times per few seconds, I would end up getting banned so often if it was set rather low ?

How high do you think you'd go with it if you were to implement it to that if you could?

(?°°)?(???? - October 12, 2016, 4:43 pm

(Oct 12, 2016 03:10 PM)ze-slade Wrote: [\[CITE\]](#) If you do limit most pages, please don't limit the new pages really low. I always click on that at least 3 times per few seconds, I would end up getting banned so often if it was set rather low ?

How high do you think you'd go with it if you were to implement it to that if you could?

Unless I'm misunderstanding the OP, he's saying you need to go to one page very very quickly (like, 10 times in one second) before you trigger it. I don't think normal browsing habits will trigger this.

Lante - October 12, 2016, 5:43 pm

(Oct 12, 2016 04:43 PM)(?°?°)?(???? Wrote: [\[CITE\]](#) Unless I'm misunderstanding the OP, he's saying you need to go to one page very very quickly (like, 10 times in one second) before you trigger it. I don't think normal browsing habits will trigger this.
Omni mentioned "12 times per minute" twice and "12 times per second" once, I think he meant 12/min, correct me if I'm wrong.

Doctor Blue - October 12, 2016, 6:19 pm

One of those features you can only test so much before you'll have to put it into production to finish testing. At least I'm not sitting at the developer end of that :)

Omniscient - October 12, 2016, 6:41 pm

Yes, it's 12 per minute. Fixed my error.

WRX - October 12, 2016, 6:43 pm

I think this will make website hit analytics more accurate. Hopefully it doesn't block me for some ungodly reason.

eCoLoGy - October 12, 2016, 11:22 pm

This is a great feature Omni!

For sites like HF with lots of users and huge databases, for sure it's a good addition to keep speeds up.

Prince™ - October 13, 2016, 7:37 am

"And seriously, disable your userscripts if you run them and you're getting blocked."

RIP user scripts users.

Cimex - October 13, 2016, 8:04 am

I got blocked yesterday. I have no idea if I refreshed like 12 times in one minute, I think I was waiting for a PM tbh.

Thanks for letting us know.

Horizon - October 13, 2016, 8:06 am

Thanks for letting us know.

Sounds like a good idea. The only page which I refresh often is the View New Posts page. But again, refreshing that more than 12 times per minute is excessive.

Cammy - October 13, 2016, 9:20 am

I tested it just for shits and giggles and i was blocked for about half an hour instead of 15 minutes
Anyways looks pretty nice addition to HF hopefully this will significantly reduce downtime even more

Omniscient - October 13, 2016, 12:48 pm

(Oct 13, 2016 09:20 AM)Cammy. Wrote: [\[CITE\]](#) I tested it just for shits and giggles and i was blocked for about half an hour instead of 15 minutes

Anyways looks pretty nice addition to HF hopefully this will significantly reduce downtime even more
I'll see if they have it set for the 15 minutes I requested.

I think 30 minutes is excessive.

Cammy - October 13, 2016, 12:51 pm

(Oct 13, 2016 12:48 PM)Omniscient Wrote: [\[CITE\]](#) I'll see if they have it set for the 15 minutes I

requested.

I think 30 minutes is excessive.

Maybe it was just something on my end with site cache or whatever, but it was certainly longer than 15 minutes.

eCoLoGy - October 13, 2016, 7:52 pm

(Oct 13, 2016 12:51 PM)Cammy. Wrote: [\[CITE\]](#) Maybe it was just something on my end with site cache or whatever, but it was certainly longer than 15 minutes.

Or maybe you don't know time? ?

Mi2414 - October 13, 2016, 7:55 pm

Haven't ran into any blocks yet, Thanks for the update Omni!

ZuGgY - October 13, 2016, 8:22 pm

Thanks for keeping us up to date (as always).

?

Cammy - October 13, 2016, 8:53 pm

(Oct 13, 2016 07:52 PM)eCoLoGy Wrote: [\[CITE\]](#) Or maybe you don't know time? ?

I'm not a smart man but I know how to read a clock.

4101 - October 14, 2016, 2:46 am

blocks access to the domain ?

can still browse other subforums by pasting direct links in the url

Armada - October 14, 2016, 7:10 am

(Oct 12, 2016 03:06 PM)Omniscient Wrote: [\[CITE\]](#) Attacks normally focus on a single attack vector. I'll be able to set rules for each page hopefully. Index page is often the target.

Reply to this really was not required, was just an observation bro.

But I do have a question.

How is this suppose to mitigate against a large scale DDoS (Such as what Krebs was recently hit with) - I mean, Ok, it will block access if a specific IP# hits a page within x / min time base, thats cool, and helpful, but how is this new protection suppose to assist against mitigated/distributed attacks? ?

Inked ?Feather - October 14, 2016, 7:13 am

nice. i was wondering why the lounge was spammed with people asking why they were banned the other day

it's a good feature if it helps with load times etc, so thanks for the update :) - do you know how long we get temp banned for if we hit the limit?

Taranis - October 14, 2016, 7:56 am

Well it's great to find out that CF is finally adding traffic control and ip ban rules, that was definitely the most important feature it had been missing and once implemented will put their protection on a whole new level.

I believe that with proper filtering rules added by user (country captcha challenge, etc) and the traffic control it will be pretty much impossible to take down a CF protected target properly setup.

I experienced some issues yesterday whenever I tried to change page. If I navigated from a thread to User Control Panel it would instantly get the ip ban error, but haven't noticed the same behavior again, seems good now !

(Oct 14, 2016 07:10 AM)Armada Wrote: [\[CITE\]](#) Reply to this really was not required, was just an observation bro.

But I do have a question.

How is this suppose to mitigate against a large scale DDoS (Such as what Krebs was recently hit with) - I mean, Ok, it will block access if a specific IP# hits a page within x / min time base, thats cool, and helpful, but how is this new protection suppose to assist against mitigated/distributed attacks? ?

Any large scale L7 DDOS would theoretically be mitigated if each IP did over xx requests to a specific page over a period of time, 1 minute in this case like Omni said.

This is a Layer 7 protection, it has nothing to do with the attacks from Mirai Botnet, although it also supports Layer 7 HTTP Floods.

Now let's see if this feature implementation will allow to set the maximum requests for both specific pages and the whole domain, otherwise it would be quite easy to circumvent as there are already bots that support multiple urls and one can also set timeouts to prevent each ip from doing over xx requests per minute.

The best protection would come from the flexibility for users to set their own rules, similarly to how you do with Nginx Rate limiting, allowing to set maximum requests over different periods of time. For instance, 12 requests in a minute is ok but ... 120 in 10 minutes is probably not and could be an indicator of a slow flood aiming to bypass such protections.

eCoLoGy - October 14, 2016, 9:46 am

(Oct 14, 2016 08:57 AM)James! Wrote: [\[CITE\]](#) I opened the index 12 times in a minute and I only got blocked from the index, I can access any other page that isn't the index whilst blocked, you might wanna fix that.

Oh.

Then the CF feature is a bit useless...

It needs to block access to the entire forum.

Omniscient - October 14, 2016, 10:02 am

Quote:How is this suppose to mitigate against a large scale DDoS (Such as what Krebs was recently hit with)

Same attack hit us 3 weeks before Krebs. Then a week afterwards it hit us twice. We were down about 5-10 minutes each time before it was mitigated. I don't really bother mentioning attacks they happen so often. At this point though so few really effect our service.

Quote:I mean, Ok, it will block access if a specific IP# hits a page within x / min time base, thats cool, and helpful, but how is this new protection suppose to assist against mitigated/distributed attacks?

That is often the style of a Layer 7 attack. Single page flood from many bots. I'm not sure what Cloudflare intends to do with this feature. I think it's a good addition though.

Quote:do you know how long we get temp banned for if we hit the limit?

I asked them to do 15 minutes but unsure if they have actually set it as such. Currently I have no interface to make any changes. They promise Restful API access before a web interface GUI.

Quote:I believe that with proper filtering rules added by user (country captcha challenge, etc) and the traffic control it will be pretty much impossible to take down a CF protected target properly setup.

Between what Cloudflare has done and my own server protections HF is very safe.

Quote:I opened the index 12 times in a minute and I only got blocked from the index
I wasn't aware it only blocked you from Index. Again, this is very early beta. There isn't even any real documentation to what they are attempting to accomplish. It is however DDOS protection name "Traffic Control". Maybe a setting for the rule to either block page or block domain will be available. I do believe they are going to offer API calls so that let's say an IP does violate a rule then I would get notified via API and I'd like respond with a block IP.

We just have to wait and see what CF does. I'm always happy to assist them.

Armada - October 14, 2016, 11:23 am

(Oct 14, 2016 07:56 AM)Taranis Wrote: [\[CITE\]](#) Any large scale L7 DDOS would theoretically be mitigated if each IP did over xx requests to a specific page over a period of time, 1 minute in this case like Omni said.

This is a Layer 7 protection, it has nothing to do with the attacks from Mirai Botnet, although it also supports Layer 7 HTTP Floods.

Now let's see if this feature implementation will allow to set the maximum requests for both specific pages and the whole domain, otherwise it would be quite easy to circumvent as there are already bots that support multiple urls and one can also set timeouts to prevent each ip from doing over xx requests per minute.

The best protection would come from the flexibility for users to set their own rules, similarly to how you do with Nginx Rate limiting, allowing to set maximum requests over different periods of time. For instance, 12 requests in a minute is ok but ... 120 in 10 minutes is probably not and could be an indicator of a slow flood aiming to bypass such protections.

IDK, I mean this is helpful along with the rest of sites security, cant argue with another level, Maybe I just dont see why such an attack/page refresh would cause such an issue.

Does CF firewalls and other safeguards already restrict this already?

This implementation only forces attackers to vary the attack vector, as Omni noted already majority of attacks hits index.php obviously. But with this implementation, all the attackers have to to is throw in a variable say index.php, verifysecret.php, etc.....

Thus bypassing the entire system just put in place, and it then just limits regular users (Who knows why they are hitting pages so fucking hard to start).

Its an added layer of protection, you wont hear no argument from me, but I fail to see how this is going to really help us....

Omniscient - October 14, 2016, 12:15 pm

Quote:Its an added layer of protection, you wont hear no argument from me, but I fail to see how this is going to really help us....

It's up to Cloudflare to implement this in a smart way and I have faith that they will. Even better they are getting my direct input.

Also note that HF already has protection against layer 7 attacks at our own server level and it's not dependent on individual pages.

HF has about 100 actual pages in the main directory. Wouldn't be hard to just put a rule in for each. Some pages should only be hit rarely so setting a low-threshold for connects would suffice.

Really, I'm just not sure on the plans CF has for Traffic Control but I assume they have a development roadmap so that it's a realistically reasonable feature to use.

Taranis - October 14, 2016, 2:25 pm

(Oct 14, 2016 11:23 AM)Armada Wrote: [CITE](#) IDK, I mean this is helpful along with the rest of sites security, cant argue with another level, Maybe I just dont see why such an attack/page refresh would cause such an issue.

Does CF firewalls and other safeguards already restrict this already?

This implementation only forces attackers to vary the attack vector, as Omni noted already majority of attacks hits index.php obviously. But with this implementation, all the attackers have to do is throw in a variable say index.php, verifysecret.php, etc.....

Thus bypassing the entire system just put in place, and it then just limits regular users (Who knows why they are hitting pages so fucking hard to start).

Its an added layer of protection, you wont hear no argument from me, but I fail to see how this is going to really help us....

To lay it out simply, imagine an attacker has 2000 bots available to attack his target.

Without any traffic control rules that will flag an IP which meets a certain criterium (in this case let's assume a maximum of 15 requests in a minute) there would only be Nginx Rate Limiting which would redirect the requests with a 503 error but still have an impact on the backend (Not saying this is HF case as Omni already mentioned that there's an extra layer of protection server side).

Now with traffic control what happens is that the maximum amount of requests possible to do from each bot the attacker has will be nerfed down to a very small amount, therefore substantially reducing the damage they can sustain.

Assuming an home connection does an average of 200 requests per second, that would be reduced to 15 requests per minute which basically means that if CF Traffic Control System did its work all the ips would be banned without much delay (threshold would be hit in the first second) and the attack would possibly not even have any effect on the backend, if it even reached backend for more than a few seconds.

Just do the maths ... even if the attacker sent a slow flood of 15 requests per minute for each ip that would mean $0.25 \text{ requests per second} \times 2000 = 500 \text{ requests per second}$, which is irrelevant.

Ofcourse if , as you said, attacked would hit multiple pages at the same time and we had 100 pages with 15 req/min then the 500 R/S would become 50000 requests/second which is already enough to cause a lot of trouble, but that's where global domain rules should come in. If you set a global rule for the domain so that each ip can't do let's say more than 30 requests in 1 minute, that would be enough to take care of it .

So yea, as you can see, a traffic control system that will ban ips and prevent them from even sending a single request to backend can be very helpful in such rare situations .

(Oct 14, 2016 12:15 PM)Omniscient Wrote: [CITE](#) It's up to Cloudflare to implement this in a smart way and I have faith that they will. Even better they are getting my direct input. Ahah they sure picked the best betatester they could have wished for ?

Quote:Really, I'm just not sure on the plans CF has for Traffic Control but I assume they have a development roadmap so that it's a realistically reasonable feature to use.

I wonder if they will provide this feature for lower tier plans, would be surprised if they did as it's typically a feature of more advanced / expensive solutions and demands a bit of high processing power to effectively mitigate hundreds / thousands of ips without delay.

ChaoticForce - October 15, 2016, 9:02 am

(Oct 14, 2016 02:25 PM)Taranis Wrote: [\[CITE\]](#) To lay it out simply, imagine an attacker has 2000 bots available to attack his target.

Without any traffic control rules that will flag an IP which meets a certain criterium (in this case let's assume a maximum of 15 requests in a minute) there would only be Nginx Rate Limiting which would redirect the requests with a 503 error but still have an impact on the backend (Not saying this is HF case as Omni already mentioned that there's an extra layer of protection server side).

Now with traffic control what happens is that the maximum amount of requests possible to do from each bot the attacker has will be nerfed down to a very small amount, therefore substantially reducing the damage they can sustain.

Assuming an home connection does an average of 200 requests per second, that would be reduced to 15 requests per minute which basically means that if CF Traffic Control System did its work all the ips would be banned without much delay (threshold would be hit in the first second) and the attack would possibly not even have any effect on the backend, if it even reached backend for more than a few seconds.

Just do the maths ... even if the attacker sent a slow flood of 15 requests per minute for each ip that would mean $0.25 \text{ requests per second} \times 2000 = 500 \text{ requests per second}$, which is irrelevant.

Ofcourse if , as you said, attacked would hit multiple pages at the same time and we had 100 pages with 15 req/min then the 500 R/S would become 50000 requests/second which is already enough to cause a lot of trouble, but that's where global domain rules should come in. If you set a global rule for the domain so that each ip can't do let's say more than 30 requests in 1 minute, that would be enough to take care of it .

So yea, as you can see, a traffic control system that will ban ips and prevent them from even sending a single request to backend can be very helpful in such rare situations .

Ahah they sure picked the best betatester they could have wished for ?

I wonder if they will provide this feature for lower tier plans, would be surprised if they did as it's typically a feature of more advanced / expensive solutions and demands a bit of high processing power to effectively mitigate hundreds / thousands of ips without delay.
if they do its a rip for you lol

b?xxy - October 15, 2016, 8:41 pm

Thanks for letting us know, I got blocked the other day and thought I was banned.
(I thought I already posted here, guess not)

J. McCarthy - October 17, 2016, 5:29 pm

Interesting stuff

Didn't know this came out

Sharjah - October 19, 2016, 1:15 am

Impressive stuff right here on Cloudflares part. Didn't even know they put this out in beta until now.

This will definitely be effective, however, I can see it being flawed for certain directories.

However, index is the perfect spot for it. Thanks Omni ?

big dick rick - October 19, 2016, 1:21 am

i sort of feel important now im part of a beta

M?xim - October 19, 2016, 1:30 am

(Oct 19, 2016 01:21 AM)big dick rick Wrote: [\[CITE\]](#) i sort of feel important now im part of a beta
Sir you are way too alpha to be in a beta test.

big dick rick - October 19, 2016, 1:31 am

(Oct 19, 2016 01:30 AM)M?xim Wrote: [\[CITE\]](#) Sir you are way too alpha to be in a beta test.
index.php me

AlphaIndustries - October 20, 2016, 5:28 am

It only blocks me from going to index.php, I still can surf the subforums

Omniscient - October 20, 2016, 12:16 pm

(Oct 20, 2016 05:28 AM)nexio Wrote: [\[CITE\]](#) It only blocks me from going to index.php, I still can surf the subforums

Yes, I think that's how they want it for now. I know it will expand to have more controls as they develop this feature. We'll just have to wait and see.

Anzee - October 21, 2016, 6:25 am

Thank goodness. All these UAM/CAPTCHA/JS bypassing L7 floods that pass through Cloudflare will now be made completely useless.

Vinnilia - October 22, 2016, 7:59 am

I tried this and I'm only banned from viewing hackforums.net but I can still view any other page on the forum.

Classicz - October 22, 2016, 12:43 pm

(Oct 12, 2016 12:50 PM)Omniscient Wrote: [\[CITE\]](#) If you've load index more than that you're access is blocked to the entire domain for 15 minutes.
Should be loaded, and your.

I'll take the Grammar Nazi Award now ?

iNviZ - October 22, 2016, 8:12 pm

Nice that is pretty cool man.

He B TeMy - October 23, 2016, 6:45 am

(Oct 22, 2016 12:43 PM)Classicz Wrote: [\[CITE\]](#) Should be loaded, and your.

I'll take the Grammar Nazi Award now ?
load should be as it is.

Ja.son - October 23, 2016, 4:01 pm

gonna test this out haaaah

QoL?? - October 23, 2016, 4:05 pm

This is a good feature. It only blocks me from index.php though. Not sure if this is intended, but I've

seen others mention it.