

Defesa de Domínio—Regras Básicas para CloudFlare WAF

[Otávio Alves](#) on 2025-10-30

Defesa de Domínio — Regras Básicas para CloudFlare WAF

Observei nesses últimos dias um **aumento** em sites públicos a utilização do **Cloudflare WAF (Firewall em Aplicativos Web)**, inclusive pela minha faculdade, entretanto, não vi **qualsquer manual ou guia** sequer da configuração básica das regras de **Firewall**, então, decidi fazer o guia básico.



Não configurei meu Dashboard, como fazer?

Neste artigo, **não é minha ideia** e provavelmente **não será por um bom tempo** em outros artigos, um guia bonito de **como fazer isso**, temos um ótimo artigo da **Hostgator** — me patrocinem — onde eles ensinam como **configurar** de maneira básica o **Dashboard**, abaixo temos um vídeo e ao final do artigo estão todos os links para realizar caso você tenha iniciado agora.



Link do vídeo:

<https://www.youtube.com/watch?v=62tV-RH7z74>

Por quais motivos precisaríamos do WAF?

Acredito que temos de começar pelo começo — *sendo lógico* — que é simplesmente: **Segurança**. Nós hoje temos um **número enorme** de ataques, como dito nesse [meu artigo aqui](#). Não podemos deixar que o mundo dos defensores seja afetado por **iniciantes** e que **falsos-positivos** apitem a todo momento, principalmente com a facilidade de hoje em dia em que os **menos experientes** apenas apertam em um botão e se consideram **Hackers**.

Agora falando sobre o **WAF** de maneira generalizada, não é nada mais que um **proxy reverso**, ou seja, um **Nginx** ou **Apache (Web Service)**, que observa por baixo dos panos a **navegação do usuário**, um exemplo, caso um usuário tente enviar uma requisição **mal-intencionada** na intenção de dar *erro no site*, o nosso querido **Firewall**, *caso configurado corretamente*, bloqueará naquele instante o usuário, impedindo que ele realize aquela ação.

Uma observação aqui, você pode utilizar o **WAF** em conjunto com um Nginx ou Apache para certas ocasiões, principalmente pela **falta de logs**, já que você precisa pagar para a **Cloudflare** caso queria ter as logs em primeira mão, o máximo que se tem é na área de “**Segurança -> Análises -> Eventos**”, onde aparece os bloqueios, challenges e qualquer atividade suspeita do usuário.

Imagem do Dashboard

na área de Regras de Segurança

Configuração básica para WAF

Vamos lá, a primeira atitude que deve se tomar é **calma**, essa configuração não servirá para todos os sistemas, você **deve** entender como funciona o **seu** sistema e se vai servir para o **seu** exemplo, **adaptabilidade é o segredo** dessa área, também vou dar um breve exemplo do porque usei isso.

Primeira Regra — Bloqueio por Geolocalização:

```
(not ip.geoip.country in {"BR"}) or (ip.geoip.country ne "BR")
```

Ação: Bloqueio Lugar na ordem: Primeiro

Imagem exemplo do

Bloqueio por Geolocalização

Por quê? Esse site em específico que estou utilizando tem como prol apenas **os usuários do Brasil** e, também, é um site *em desenvolvimento*, então não há motivos para liberar acessos de fora pelo momento.

Segunda Regra — Diretórios Proibidos:

```
(http.request.uri.path contains "admin") or (http.request.uri.path contains "etc") or (http.request.uri.path contains "passwd")
```

Ação: Block/Challenge Lugar na ordem: Customizado (Segundo)

The screenshot shows the CloudFlare WAF rule editor interface. The rule is titled "Diretórios Proibidos" (Blocked Directories). It contains three "Or" conditions under "When incoming requests match...":

- URI Path contains "admin" (e.g. /content)
- URI Path contains "etc" (e.g. /content)
- URI Path contains "passwd" (e.g. /content)

The "Then take action..." section includes a "Choose action" dropdown set to "Block", which is described as "Blocks matching requests and stops evaluating other rules". The "Place at" section is set to "Custom".

Expression Preview: `(http.request.uri.path contains "admin") or (http.request.uri.path contains "etc") or (http.request.uri.path contains "passwd")`

Imagem exemplo do Bloqueio de Diretórios

Bloqueio de Diretórios

Por quê? Nesse caso, **verifiquei** nas atividades enquanto estava no painel, que a maior parte dos **atacantes** utilizavam esses valores em seus ataques utilizando *Gobuster/Dirbuster*, foram poucas regras apenas para ter um bloqueio básico.

Terceira Regra — Proteção contra Brute-Force:

`(http.request.uri.path contains "login" and http.request.method eq "POST")`

Ação: Challenge Lugar na ordem: Customizado (Terceiro)

The screenshot shows the CloudFlare WAF rule editor interface. The rule is titled "When incoming requests match...". It contains two conditions under "And":

- URI Path contains "login" (e.g. /content)
- Request Method equals "POST" (e.g. GET)

The "Then take action..." section includes a "Choose action" dropdown set to "Managed Challenge", which is described as "Presents an interactive or non-interactive challenge to the client". The "Place at" section is set to "Custom".

Expression Preview: `(http.request.uri.path contains "login" and http.request.method eq "POST")`

Imagem exemplo de Proteção contra Brute Force

Por quê? O site possui um **sistema de login** já no início do site e, como peguei o projeto na metade do caminho, havia percebido que os usuários de fora tentavam enviar **requisições POST** na intenção de entrar e ganhar acesso administrativo por meio de ferramentas como *Hydra/John the Ripper*, uma observação, apenas nesse **endpoint** tem sistema de login e não é possível mexer em nada do site por dentro.

Quarta Regra — Regras genéricas:

`(http.user_agent contains "(http.user_agent contains \"curl\" or http.user_agent contains \"python-requests\" or http.user_agent contains \"wget\") or`

Ação: Challenge Lugar na Ordem: Último

Regras Genéricas
Give your rule a descriptive name.

When incoming requests match...

Field	Operator	Value
User Agent	contains	(http.user_agent contains "curl" or http.user_agent contains "python-requests" or http.user_agent contains "sqlmap" or http.user_agent contains "nmap" or http.user_agent contains "masscan") e.g. Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6)...

Expression Preview [Edit expression](#)

```
(http.user_agent contains "(http.user_agent contains \"curl\" or http.user_agent contains \"python-requests\" or http.user_agent contains \"sqlmap\" or http.user_agent contains \"nmap\" or http.user_agent contains \"masscan\")")
```

Then take action...

Choose action: **JS Challenge**
Presents a JavaScript challenge to the client making the request.

Place at: **Custom**

☒ Imagem exemplo de

Regras Genéricas

Por quê? Nesse caso em específico, percebi que havia **diversas** requisições sobre “User Agent” e “Headers” modificados, com ferramentas básicas no mercado atrapalhando os logs com **falsos-positivos**, então foi meu método de aproveitar os erros deles e tirar uma parte dos problemas.

Quinta regra — Proteção DDoS/Flood:

(http.request.uri.path wildcard "*")

Requisições: 200 em 10 segundos **Ação:** Block **Lugar na Ordem:** Primeiro/Último

Expression Preview [Edit expression](#)

```
(http.request.uri.path wildcard "")
```

With the same characteristics...

IP

When rate exceeds...

Requests (required) **200** Period (required) **10 seconds**

Then take action...

Choose action: **Block**
Blocks matching requests and stops evaluating other rules

☒ Imagem exemplo de

Rate Limiting

Por quê? Me permita explicar *antes que os especialistas me batam*, **Cloudflare WAF Free Plan** tem um limite, só tem como pôr **10 segundos** por uma certa quantidade de *requests* e, como eu disse lá no início, é apenas um exemplo, apenas para **bloquear** uma quantidade absurda em segundos, já é a segunda vez que nesse site houve um **ataque DDoS**, com essa regra, não houve derrubada e o ataque foi completamente anulado.

Configurações de Segurança da Cloudflare:

Sinto que muitas pessoas *novas* no ambiente da **Cloudflare WAF** terão problemas com outras coisas durante a **proteção de site**, com isso eu cito **DDoS** na maioria dos casos.

Para prevenir isso, o **WAF** também possui na área de Configurações em “**Segurança**”, com filtragem de configurações para cada tipo de problema.

The screenshot shows the Cloudflare Settings interface. On the left, there's a sidebar with various sections like AI Crawl Control, Log Explorer, Analytics & logs, DNS, Email, SSL/TLS, Security (which is expanded), and more. The 'Security' section is currently selected. The main area is titled 'Settings' and contains a message about the 'New application security dashboard'. It includes a toggle switch that is turned on, a link to 'Learn more about the new experience', a 'Feedback' link, and two tabs: 'General' and 'Dashboard version'. At the bottom of the page, there's a 'Switch to old sidebar' button.

↳ Tela de Configuração

de Segurança

Você pode **configurar** desde o *domínio* até as *ferramentas de detecção*, aplicando cada uma delas da sua forma, desde que não exagere, a aplicação fica mais segura e mais utilizável.

Cloudflare não fará tudo por você, a segurança deve ser feita de maneira *automatizada*, mas também *manual* na maioria dos casos, não dependa desse tipo de ferramenta.

Finalização do Conteúdo

Tentei deixar esse artigo **o mais simples possível**, até mesmo para as pessoas que entendem pouco de *computação* e até mesmo *segurança* consigam **entender** pelo menos o **essencial** do artigo, **sempre** vou prezar pelo **nível técnico**, mas se outras pessoas fora *não conseguem entender*, não me vale de fazer esse tipo de artigo.

Uma observação durante esse texto, para quem gosta **realmente** de entender *como funciona*, deixei um “**erro**” que não afeta em nada enquanto estava fazendo o artigo, apenas **dupliquei** um **artefato**, mas ficaria muito feliz caso achassem, **uma dica**, está em uma das regras.

Enfim, **apliquem essas regras** de acordo com a sua necessidade, façam o favor de não dar um *Ctrl + C* e *Ctrl + V* sem entender **as funções por trás**, talvez elas nem sirvam pra você, o **desempenho pode alterar** um pouco sem necessidade de tal.

Recomendo que leiam meu último artigo: [Esse aqui](#) e também me acompanhem no **LinkedIn**, por mais que *eu não tenha mais vontade nenhuma de postar na plataforma*, ainda assim é bom ter uma movimentação básica lá.

<https://www.linkedin.com/in/otavio-alves/>

Até uma próxima.

Referências:

Guia: aprenda a configurar a Cloudflare em seu site Aprenda a configurar seu site na Cloudflare para aproveitar diversas ferramentas gratuitas dessa plataforma! Tempo... www.hostgator.com.br

O que é a Cibersegurança Vemos cada vez mais que citamos sobre a segurança cibernética de maneira geral, citamos sobre as formas de defesa e... medium.com

Custom rules · Cloudflare Web Application Firewall (WAF) docs Custom rules allow you to control incoming traffic by filtering requests to a zone. They work as customized web... developers.cloudflare.com