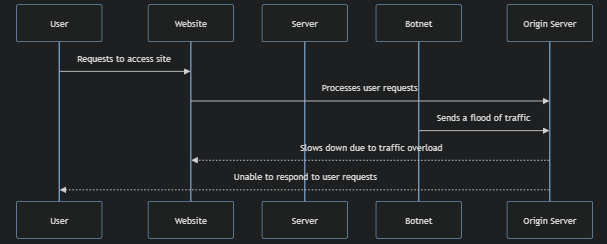
**Modun 5 Bảo vệ**

Khi bản ghi DNS của bạn được proxy thông qua Cloudflare, Cloudflare cung cấp khả năng bảo vệ DDoS miễn phí và không giới hạn cùng các biện pháp bảo vệ khác thông qua Tường lửa ứng dụng web (WAF).

**Bảo vệ DDoS**

Tấn công từ chối dịch vụ phân tán (DDoS) là khi một số lượng lớn máy tính hoặc thiết bị, thường do một kẻ tấn công duy nhất kiểm soát, cố gắng truy cập vào một trang web hoặc dịch vụ trực tuyến cùng một lúc. Lũ lưu lượng truy cập này có thể làm quá tải máy chủ gốc của trang web, khiến trang web chậm lại hoặc thậm chí bị sập. 

**Bộ quy tắc được quản lý**

Tất cả khách hàng đều có quyền truy cập vào Cloudflare Free Managed Ruleset, cung cấp các biện pháp giảm thiểu các lỗ hổng bảo mật nghiêm trọng và có tác động rộng.

***Để biết thêm chi tiết, hãy tham khảo tài liệu WAF .***

**Cài đặt SSL/TLS**

**Chế độ mã hóa**

Chế độ mã hóa SSL/TLS của vùng của bạn kiểm soát cách Cloudflare quản lý hai kết nối: một kết nối giữa khách truy cập và Cloudflare, và kết nối còn lại giữa Cloudflare và máy chủ gốc của bạn.



**Thiết lập cơ bản**

Cách đơn giản nhất để chọn chế độ mã hóa là bật SSL/TLS Recommender , công cụ này sẽ quét tên miền của bạn và đề xuất cài đặt phù hợp.

Để đảm bảo bạn không vô tình chặn SSL/TLS Recommender , hãy xem lại cài đặt để đảm bảo tên miền của bạn:

* Có thể truy cập được.
* Không chặn các yêu cầu từ bot của chúng tôi (sử dụng tác nhân người dùng của Cloudflare-SSLDetector).
* Không có bất kỳ Quy tắc trang hoặc quy tắc cấu hình nào dành riêng cho SSL .

Sau đó, bạn có thể bật khuyến nghị SSL/TLS trong bảng điều khiển:

Đăng nhập vào bảng điều khiển Cloudflarevà chọn tài khoản và ứng dụng của bạn.

Đi tới SSL/TLS .

Đối với SSL/TLS Recommender , hãy chuyển nút gạt sang vị trí Bật .

Sau khi được bật, SSL/TLS Recommender sẽ chạy quét nguồn gốc bằng tác nhân người dùng Cloudflare-SSLDetectorvà bỏ qua robots.txttệp của bạn (trừ các quy tắc nhắm mục tiêu rõ ràng vào tác nhân người dùng).

Dựa trên lần quét ban đầu này, Recommender có thể quyết định rằng bạn có thể sử dụng chế độ mã hóa SSL mạnh hơn . Nó sẽ không bao giờ đề xuất tùy chọn yếu hơn tùy chọn hiện đang được cấu hình.

Nếu vậy, nó sẽ gửi cho chủ sở hữu ứng dụng một email có tùy chọn được đề xuất và thêm thẻ Được Cloudflare đề xuất vào tùy chọn đó trên trang SSL/TLS . Bạn không bắt buộc phải sử dụng khuyến nghị này.

Nếu bạn không nhận được email, hãy giữ nguyên chế độ mã hóa SSL hiện tại .

​​**Thiết lập an toàn**

Nếu có thể, Cloudflare khuyên bạn nên sử dụng chế độ Đầy đủ hoặc Đầy đủ (nghiêm ngặt) để ngăn chặn các kết nối độc hại đến nguồn gốc của bạn.

Những chế độ này thường yêu cầu thiết lập bổ sung và có thể khó khăn hơn về mặt kỹ thuật.

​​**Thực thi kết nối HTTPS**

Ngay cả khi ứng dụng của bạn có chứng chỉ edge đang hoạt động, khách truy cập vẫn có thể truy cập tài nguyên qua kết nối HTTP không an toàn.

Tuy nhiên, bằng cách sử dụng nhiều cài đặt Cloudflare khác nhau, bạn có thể buộc tất cả hoặc hầu hết các kết nối của khách truy cập sử dụng HTTPS .

​​**Đánh giá các tính năng bổ sung**

Sau khi bạn đã chọn chế độ mã hóa và áp dụng kết nối HTTPS, hãy đánh giá các cài đặt sau:

**Chứng chỉ Edge :** Tùy chỉnh các khía cạnh khác nhau của chứng chỉ Edge, từ việc bật Mã hóa cơ hội đến chỉ định Phiên bản TLS tối thiểu .

**Xác thực nguồn gốc :** Đảm bảo mọi yêu cầu đến máy chủ gốc của bạn đều xuất phát từ mạng Cloudflare.

**Thông báo :** Thiết lập cảnh báo liên quan đến trạng thái xác thực chứng chỉ, việc cấp, triển khai, gia hạn và hết hạn.

**Chế độ chiến đấu của Bot**

Bot Fight Mode là một sản phẩm đơn giản, miễn phí giúp phát hiện và giảm thiểu lưu lượng bot trên miền của bạn. Khi được bật, sản phẩm:

* Xác định các mẫu khớp lưu lượng truy cập của các bot đã biết
* Các vấn đề thách thức tốn kém về mặt tính toán để đáp ứng với các bot này
* Thông báo cho Bandwidth Allianceđối tác (nếu có) để vô hiệu hóa bot

​​**Những cân nhắc**

Chế độ chiến đấu của Bot có một số hạn chế, bao gồm:

* Bảo vệ toàn bộ miền mà không có giới hạn điểm cuối.
* Không thể tùy chỉnh, điều chỉnh hoặc cấu hình lại thông qua các quy tắc tùy chỉnh WAF .

Nếu những hạn chế này có thể gây ra sự cố cho ứng dụng của bạn, đừng bật tính năng này.

Để kiểm soát chi tiết hơn - bao gồm khả năng sử dụng Skiphành động để giảm thiểu bot - hãy cân nhắc sử dụng Chế độ chiến đấu siêu bot .

**​​Cài đặt**

1. Đăng nhập vào bảng điều khiển Cloudflarevà chọn tài khoản và tên miền của bạn.
2. Vào Bảo mật > Bot .
3. Đối với Chế độ chiến đấu với Bot , hãy chọn Bật .

**Kết nối nguồn gốc an toàn**

Khi bạn bảo mật các kết nối gốc, điều này sẽ ngăn chặn kẻ tấn công phát hiện và làm quá tải máy chủ gốc của bạn bằng các yêu cầu.

**DNS :**

* Bản ghi proxy (nếu có thể): Thiết lập bản ghi DNS proxy (màu cam-mây) để ẩn địa chỉ IP gốc của bạn và cung cấp khả năng bảo vệ DDoS. Là một phần của việc này, bạn nên cho phép địa chỉ IP Cloudflare tại nguồn gốc của mình để ngăn chặn các yêu cầu bị chặn.
* Xem lại các bản ghi chỉ dành cho DNS : Kiểm tra các bản ghi chỉ dành cho DNS hiện có ( SPF, TXT, v.v.) để đảm bảo chúng không chứa thông tin IP gốc.
* Đánh giá cơ sở hạ tầng thư : Nếu có thể, đừng lưu trữ dịch vụ thư trên cùng máy chủ với tài nguyên web mà bạn muốn bảo vệ, vì email được gửi đến địa chỉ không tồn tại sẽ bị trả lại cho kẻ tấn công và tiết lộ IP của máy chủ thư.
* Xoay vòng IP gốc : Sau khi đã đăng ký , hãy xoay vòng IP gốc của bạn vì bản ghi DNS nằm trong phạm vi công cộng. Bản ghi lịch sử được lưu giữ và sẽ chứa địa chỉ IP trước khi tham gia Cloudflare.

**Trung tâm bảo vệ**

Cloudflare Security Center kết hợp bộ sản phẩm bảo mật, chuyên môn bảo mật và trí thông minh Internet độc đáo của chúng tôi thành một giải pháp trí thông minh bảo mật thống nhất. Security Center cho phép bạn tăng cường thế trận bảo mật của mình bằng cách:

* Lập bản đồ bề mặt tấn công mạng của bạn
* Cung cấp kiểm kê và khám phá tài sản
* Xác định các rủi ro bảo mật tiềm ẩn, cấu hình sai và lỗ hổng
* Giúp bạn giảm thiểu những rủi ro này thông qua việc khắc phục chỉ bằng vài cú nhấp chuột

Để biết thêm thông tin chi tiết và trợ giúp, hãy tham khảo tài liệu Trung tâm bảo mật .

​​**Cài đặt**

Để bật Security Insights và thực hiện quét bảo mật ban đầu:

1. Đăng nhập vào bảng điều khiển Cloudflarevà chọn tài khoản của bạn.
2. Trong Trang chủ tài khoản, hãy vào Trung tâm bảo mật > Thông tin chi tiết về bảo mật .
3. Trong mục Bật quét Trung tâm bảo mật , hãy chọn Bắt đầu quét .

Quá trình quét Security Insights ban đầu sẽ bắt đầu. Thời gian quét ban đầu phụ thuộc vào số lượng tài sản CNTT trong tất cả các miền của tài khoản Cloudflare của bạn. Khi quá trình quét hoàn tất, trạng thái của trang sẽ thay đổi từ Đang quét thành Lần quét cuối cùng được thực hiện trên:<DATE\_TIME> .

**Cài đặt hệ thống bảo vệ**

Ngoài những cải tiến mặc định, SSL/TLS và DNSSEC, Cloudflare cho phép tất cả khách hàng điều chỉnh các cài đặt sau để cải thiện bảo mật trang web.

​​**Bảo vệ**

Trong phần bảo mậtcủa bảng điều khiển Cloudflare, hãy xem lại các cài đặt sau:

* Quy tắc tùy chỉnh WAF
* Quy tắc giới hạn tỷ lệ
* Quy tắc truy cập IP
* Quy tắc chặn tác nhân người dùng
* Nhiều thiết lập bảo mật khác nhau

​​**Lá chắn cạo**

Trong phần Scrape Shieldcủa bảng điều khiển Cloudflare, hãy xem lại các cài đặt sau:

* Làm mờ địa chỉ email
* Bảo vệ Hotlink