**Modun 3 Thêm tên miền của bạn vào Cloudflare**

**Giảm thiểu thời gian chết**

Khi thực hiện bất kỳ thay đổi nào đối với định tuyến của ứng dụng Internet, luôn có khả năng xảy ra tình trạng ngừng hoạt động do cấp chứng chỉ, cài đặt cấu hình sai hoặc hạn chế tại máy chủ gốc của bạn. Để tránh tình trạng ngừng hoạt động khi đưa vào hoạt động, điều quan trọng là phải xem xét các cấu hình phổ biến nhất.

​​**Cập nhật và xem lại bản ghi DNS.**

Trước khi kích hoạt tên miền của bạn trên Cloudflare (các bước chính xác phụ thuộc vào thiết lập DNS của bạn ), hãy xem lại bản ghi DNS trong tài khoản Cloudflare của bạn.

​​Bắt đầu với các bản ghi không được ủy quyền

Với tên miền mới, hãy đảm bảo tất cả bản ghi DNS của bạn đều có trạng thái proxy là DNS-only.

Cài đặt này ngăn Cloudflare chuyển tiếp lưu lượng truy cập của bạn trước khi bạn có chứng chỉ biên đang hoạt động hoặc trước khi bạn cho phép địa chỉ IP của Cloudflare.

​​Xác nhận độ chính xác của hồ sơ

Hãy dành thêm thời gian để xác nhận tính chính xác của bản ghi DNS trước khi kích hoạt tên miền của bạn, đặc biệt chú ý đến:

Bản ghi đỉnh vùng ( example.com)

Bản ghi tên miền phụ ( www.example.comhoặc blog.example.com)

Hồ sơ email

Nếu bạn thêm bản ghi DNS vào nhà cung cấp DNS có thẩm quyền của mình giữa thời điểm đưa tên miền lên mạng và kích hoạt tên miền, bạn cũng có thể cần thêm các bản ghi này trong Cloudflare.

​​**Kích hoạt tên miền của bạn.**

Hoàn tất thiết lập DNS cho tên miền của bạn, chuyển trạng thái tên miền sang Hoạt động :

Thiết lập đầy đủ : Cập nhật máy chủ tên có thẩm quyền tại cơ quan đăng ký tên miền của bạn và đợi thay đổi đó được xác thực.

Thiết lập một phần : Thêm bản ghi TXT xác minh vào DNS có thẩm quyền của bạn và đợi thay đổi đó được xác thực.

​​**Xác minh chứng chỉ SSL/TLS.**

Trước khi ủy quyền lưu lượng truy cập của bạn thông qua Cloudflare, hãy xác minh rằng Cloudflare có Chứng chỉ Edge đang hoạt động cho tên miền của bạn.

Để biết thêm chi tiết về thời gian và khuyến nghị cấp chứng chỉ, hãy tham khảo mục Cấp chứng chỉ .

​​**Cấu hình thử nghiệm.**

Bạn có thể muốn kiểm tra cấu hình của mình bằng máy cục bộ hoặc lưu lượng truy cập proxy từ miền phát triển hoặc miền phụ.

Nếu bạn gặp sự cố, bạn nên đảm bảo rằng bạn đã cho phép địa chỉ IP Cloudflare tại máy chủ gốc của mình.

​​**Cập nhật trạng thái proxy.**

Sau khi xác minh rằng chứng chỉ SSL/TLS của bạn đang hoạt động và bạn đã cho phép địa chỉ **Cho phép địa chỉ IP Cloudflare**

Tất cả lưu lượng truy cập đến các bản ghi DNS được proxy đều đi qua Cloudflare trước khi đến máy chủ gốc của bạn. Điều này có nghĩa là máy chủ gốc của bạn sẽ ngừng nhận lưu lượng truy cập từ các địa chỉ IP của từng khách truy cập và thay vào đó nhận lưu lượng truy cập từ các địa chỉ IP của Cloudflare, được chia sẻ bởi tất cả các tên máy chủ được proxy.

Thiết lập này có thể gây ra sự cố nếu máy chủ gốc của bạn chặn hoặc giới hạn tốc độ kết nối từ địa chỉ IP Cloudflare. Vì tất cả lưu lượng truy cập của khách truy cập sẽ xuất hiện từ địa chỉ IP Cloudflare, việc chặn các IP này — ngay cả khi vô tình — sẽ ngăn lưu lượng truy cập của khách truy cập đến ứng dụng của bạn.

Ngoài ra, có thể cần phải cho phép IP Cloudflare để tránh giới hạn tốc độ hoặc chặn các yêu cầu này tại máy chủ gốc của bạn.

Đối với khách hàng Magic Transit , Cloudflare định tuyến lưu lượng thay vì proxy. Khi Cloudflare bắt đầu quảng cáo tiền tố IP của bạn, nó sẽ chấp nhận các gói IP được định tuyến đến mạng của bạn, xử lý chúng và sau đó xuất các gói này đến cơ sở hạ tầng gốc của bạn.

​​**Xem lại các công cụ bên ngoài**

Để tránh vô tình chặn địa chỉ IP của Cloudflare, hãy xem lại các công cụ bên ngoài để kiểm tra rằng:

Bất kỳ plugin bảo mật nào — chẳng hạn như plugin dành cho WordPress — đều cho phép sử dụng địa chỉ IP của Cloudflare.

Bản mod\_securityplugin đã được cập nhật.

​​**Cấu hình máy chủ gốc**

​​**Cho phép địa chỉ IP Cloudflare**

Để tránh vô tình chặn địa chỉ IP của Cloudflare, bạn cũng nên cho phép địa chỉ IP của Cloudflare tại máy chủ web gốc của mình.

Bạn có thể cho phép rõ ràng các địa chỉ IP này bằng tệp .htaccesshoặc bằng cách sử dụng iptables.

Ví dụ sau đây minh họa cách bạn có thể sử dụng quy tắc iptables để cho phép phạm vi địa chỉ IP của Cloudflare. Thay thế $ipbên dưới bằng một trong các phạm vi địa chỉ IP của Cloudflare.

# For IPv4 addresses

$ iptables -I INPUT -p tcp -m multiport --dports http,https -s $ip -j ACCEPT

# For IPv6 addresses

$ ip6tables -I INPUT -p tcp -m multiport --dports http,https -s $ip -j ACCEPT

Để được hướng dẫn cụ thể hơn, hãy liên hệ với nhà cung cấp dịch vụ lưu trữ hoặc quản trị viên trang web của bạn.

​​**Chặn các địa chỉ IP khác (khuyến nghị)**

Theo thông lệ tốt nhất, chúng tôi cũng khuyên bạn nên chặn rõ ràng mọi lưu lượng truy cập không đến từ địa chỉ IP của Cloudflare hoặc địa chỉ IP của các đối tác, nhà cung cấp hoặc ứng dụng đáng tin cậy của bạn.

Ví dụ, bạn có thể cập nhật iptables của mình với các lệnh sau:

iptables -A INPUT -p tcp -m multiport --dports http,https -j DROP

ip6tables -A INPUT -p tcp -m multiport --dports http,https -j DROP

**Vô hiệu hóa DNSSEC**

Tiện ích mở rộng bảo mật DNS (DNSSEC) bổ sung thêm một lớp xác thực vào DNS, đảm bảo các yêu cầu không được chuyển hướng đến một tên miền giả mạo.

Nếu bạn đang đưa một tên miền hiện có lên Cloudflare, hãy đảm bảo DNSSEC đã bị vô hiệu hóa tại đơn vị đăng ký của bạn (nơi bạn mua tên miền). Nếu không, tên miền của bạn sẽ gặp lỗi kết nối khi bạn thay đổi máy chủ tên.

*Khi tên miền của bạn đã bật DNSSEC, nhà cung cấp DNS của bạn sẽ ký số tất cả các bản ghi DNS của bạn. Hành động này ngăn chặn bất kỳ ai khác phát hành các bản ghi DNS sai thay mặt bạn và chuyển hướng lưu lượng truy cập dành cho tên miền của bạn.*

*Tuy nhiên, việc có một bộ bản ghi đã ký duy nhất cũng ngăn Cloudflare cấp bản ghi DNS mới thay mặt bạn (đây là một phần của việc sử dụng Cloudflare cho máy chủ tên có thẩm quyền của bạn). Vì vậy, nếu bạn thay đổi máy chủ tên mà không tắt DNSSEC, DNSSEC sẽ ngăn các bản ghi DNS của Cloudflare giải quyết đúng cách.*

**Thêm một trang web**

* Đăng nhập vào bảng điều khiển Cloudflare.
* Trên thanh điều hướng trên cùng, chọn Thêm trang web .
* Nhập tên miền chính của trang web của bạn ( example.com) rồi chọn Tiếp tục .

Nếu Cloudflare không thể xác định tên miền của bạn là tên miền đã đăng ký, hãy đảm bảo bạn đang sử dụng tên miền cấp cao nhất hiện có( .com, .net, .biz, hoặc các tên khác).

Ngoài ra, Cloudflare yêu cầu tên miền của bạn apex domainphải thấp hơn một cấp so với TLD hợp lệ được xác định trong Danh sách hậu tố công khai (PSL).

**Chọn mức gói của bạn.** Để biết thêm chi tiết về các tính năng và giá cả, hãy tham khảo trang Gói của chúng tôi.

**Xem lại hồ sơ DNS của bạn.**

Khi bạn thêm một trang web mới vào Cloudflare, Cloudflare sẽ tự động quét các bản ghi chung và thêm chúng vào vùng DNS. Các bản ghi sẽ hiển thị trong trang DNS > Bản ghi vùng tương ứng .

Vì quá trình quét này không đảm bảo tìm thấy tất cả các bản ghi DNS hiện có nên bạn cần xem lại hồ sơ của mình, đặc biệt chú ý đến các loại bản ghi sau:

* Bản ghi đỉnh vùng ( example.com)
* Bản ghi tên miền phụ ( www.example.comhoặc blog.example.com)
* Hồ sơ email

Nếu bạn kích hoạt tên miền của mình trên Cloudflare mà không thiết lập đúng bản ghi DNS cho tên miền và tên miền phụ, khách truy cập của bạn có thể gặp lỗi DNS\_PROBE\_FINISHED\_NXDOMAIN .

Nếu bạn tìm thấy bất kỳ bản ghi nào bị thiếu, hãy thêm các bản ghi đó theo cách thủ công.

Tùy thuộc vào thiết lập trang web của bạn, bạn có thể muốn điều chỉnh trạng thái proxy cho một số bản ghi A, AAAA, hoặc CNAME.

Chọn Tiếp tục .