Giới hạn IP truy cập trên Ingress Nginx

**1. Vấn đề**

* Có một vài domain cần giới hạn truy cập , chỉ cho phép các dải mạng từ công ty có quyền truy cập đến để sử dụng, không có nhu cầu public ra ngoài
* Giảm thiểu rủi ro về bảo mật cũng như  phòng chống việc bị tấn công từ mạng bên ngoài, bảo vệ dữ liệu khỏi những truy cập trái phép

**2. Muc tiêu và giải pháp**

* Tạo ra 1 whitelist IP cho những domain cần giới hạn truy cập để chỉ những IP đó mới có thể truy cập được
* Liên tục cập nhật danh sách whitelist IP khi có sự thay đổi để tránh gián đoạn khi dùng

**3. Thực hiện**

* **Bước 1 : Tổng hợp danh sách Whitelist IP cho domain cần giới hạn truy cập**- Dưới đây là danh sách IP Public từ dưới văn phòng HN

14.177.239.192

101.99.7.132

101.99.7.213

14.177.239.244

183.91.4.105

14.177.239.203

         - Dưới đây là danh sách IP Public từ dưới văn phòng HCM

118.69.34.233

113.161.48.116

Về cơ bản tối thiểu , chúng ta chỉ cần thêm những IP trên để giới hạn truy cập và chỉ cho phép truy cập từ dưới văn phòng. Nếu muốn cho các dịch vụ khác ở dưới DC gọi lên thì có thể add thêm

* **Bước 2 : Thêm Whitelist IP cho Ingress Nginx để chỉ cho phép những IP này truy cập**

 - Ta tiến hành cấu hình annotation của ingress nginx theo cú pháp sau :

Trong đó

annotations:

nginx.ingress.kubernetes.io/configuration-snippet: |

set\_real\_ip\_from 10.0.0.0/8;

real\_ip\_header X-Forwarded-For;

nginx.ingress.kubernetes.io/whitelist-source-range: 14.177.239.192/32,101.99.7.132/32,101.99.7.213/32,14.177.239.244/32,183.91.4.105/32,14.177.239.203/32,118.69.34.233/32,113.161.48.116/32

1. **nginx.ingress.kubernetes.io/configuration-snippet**:
   * Annotation này cho phép bạn thêm các đoạn mã cấu hình tùy chỉnh trực tiếp vào cấu hình Nginx.
   * set\_real\_ip\_from 10.0.0.0/8;: Thiết lập địa chỉ IP thực tế khi sử dụng một proxy truyền thông tin từ phía trước Nginx. Trong trường hợp này, nó cho phép truyền thông tin IP thực tế từ các địa chỉ IP thuộc dải 10.0.0.0/8.
   * real\_ip\_header X-Forwarded-For;: Xác định rằng thông tin IP thực tế được chuyển tiếp qua HTTP header "X-Forwarded-For". Điều này là quan trọng khi Nginx đứng sau một proxy hoặc load balancer.
2. **nginx.ingress.kubernetes.io/whitelist-source-range**:
   * Annotation này được sử dụng để giới hạn truy cập đến Ingress Controller từ các địa chỉ IP cụ thể.
   * Trong trường hợp này, chỉ có hai địa chỉ IP được phép truy cập: 14.177.239.192 và 101.99.7.132. Cả hai đều là địa chỉ IP đơn (CIDR /32, chỉ là một địa chỉ cụ thể).

**Bổ sung thêm:**

- Trong 1 vài trường hợp đặc biệt , có domain muốn dùng tài nguyên ví dụ như ảnh,file tĩnh từ 1 domain khác,  cần cấu hình annotations để cho phép từ 1 domain khác có thể truy cập được tài nguyên ta làm như sau :

Giả sử trên trang web [https://alepay-merchant.nganluong.vn](https://alepay-merchant.nganluong.vn/) muốn lấy file font chữ css trên trang [https://static-alepay.nganluong.vn](https://static-alepay.nganluong.vn/) thì trong cấu hình annotations của ingress nginx của domain static.alepay.nganluong.vn ta thêm như sau :

1

annotations:

nginx.ingress.kubernetes.io/enable-cors: "true"

nginx.ingress.kubernetes.io/cors-allow-origin: "https://alepay-merchant.nganluong.vn"