Ví dụ về Standard access-list trên Router Cisco

Cấu hình một số access-list để tôi có thể trình bày cách thực hiện trên Cisco IOS Router. Trong bài này chúng ta sẽ đề cập đến Standard access-list. Đây là mô hình:







Hai router và mỗi router có loopback interface. Tôi sẽ sử dụng hai định tuyến tĩnh để hai router có thể giao tiếp loopback interface của nhau:

! Nếu sử dụng giao thức định tuyến để quảng cáo mạng, hãy cẩn thận để access-list không chặn lưu lượng RIP, EIRP hoặc OSPF…

Bây giờ, chúng ta sẽ bắt đầu với một ACL Standard. Tôi sẽ tạo một ACL trên R2 chỉ cho phép lưu lượng từ mạng 192.168.12.0/24:



Chỉ cần một "permit" duy nhất này là đủ và cuối ACL luôn có một lệnh "deny any". Nó không hiển thị trên màn hình nhưng nó luôn tồn tại. Áp dụng ACL này vào luồng dữ liệu inbound trên R2:

Sử dụng lệnh **ip access-group** để áp dụng danh sách này vào một interface. Áp dụng nó cho luồng dữ liệu inbound với từ khóa "in".





Có thể xác nhận rằng ACL đã được áp dụng bằng cách sử dụng lệnh **show ip interface**. Ở trên, ta thấy rằng access-list 1 đã được áp dụng cho inbound.

Bây giờ, chúng ta hãy tạo một số lưu lượng...



Ping của chúng ta đã thành công; hãy kiểm tra ACL:



Như bạn thấy, access-list hiển thị số lượng kết quả khớp cho mỗi dòng lệnh. Chúng ta có thể sử dụng thông tin này để xác minh access-list của mình



Khi bạn gửi một lệnh ping, bạn có thể sử dụng từ khóa **source** để chọn interface. Địa chỉ IP nguồn của gói tin bây giờ là 1.1.1.1, và bạn có thể thấy các lệnh ping này không thành công vì ACL (Access Control List - danh sách điều khiển truy cập) đã chặn chúng



Bạn sẽ không thấy chúng với lệnh **show access-list** vì lệnh **deny any** đang chặn chúng.

Giờ ta sẽ chặn lưu lượng từ mạng 192.168.12.0/24 nhưng cho phép tất cả các mạng khác. Ta có thể làm như sau:



Ta sẽ tạo một ACL mới và lệnh đầu tiên sẽ chặn mạng 192.168.12.0/24. Lệnh thứ hai sẽ cho phép tất cả. Vì lệnh cho phép **permit any** này, không có gì sẽ đi vào lệnh **deny any** vô hình, ngoại trừ mạng 192.168.12.0/24. Hãy áp dụng ACL mới này:



Bây giờ nó đã hoạt động, hãy thử kiểm tra:





Những gói tin ping này đang chạm vào dòng lệnh đầu tiên và bị chặn....





Và những gói tin ping từ giao diện loopback0 của R1 đang chạm vào dòng lệnh thứ hai và được phép truyền qua.

Nếu tôi muốn xóa một dòng lệnh từ danh sách điều khiển truy cập (ACL), bạn sẽ gặp một bất ngờ thú vị:



Giả sử tôi muốn xóa dòng lệnh trên. Tôi sẽ gõ **no access-list** và đây là những gì bạn sẽ thấy:



Toàn bộ danh sách điều khiển truy cập (ACL) đã biến mất... Bạn không thể sử dụng no access-list để xóa một dòng lệnh. Router của bạn sẽ chỉ chấp nhận lệnh no access-list 2 và xóa toàn bộ ACL. Điều này thú vị khi thử nghiệm trong phòng lab, nhưng không vui chút nào trên mạng sản xuất.

Ngoài việc áp dụng ACL cho lưu lượng vào (inbound) hoặc ra (outbound), bạn cũng có thể áp dụng nó cho các dòng VTY (Telnet/SSH). Điều này hữu ích nếu bạn muốn bảo mật quyền truy cập Telnet hoặc SSH vào router. Hãy cấu hình R1 để chỉ cho phép truy cập Telnet từ mạng 192.168.12.0/24:



Ở trên, bạn có thể thấy tôi đã tạo ACL số 3, nhưng tôi sử dụng lệnh access-class trên các dòng VTY. Trên các interface, chúng ta sử dụng lệnh access-group, nhưng trên các dòng VTY, bạn cần sử dụng lệnh access-class để áp dụng chúng.

Hãy thử sử dụng lệnh Telnet:



Thông báo hiện lên "open", có nghĩa là kết nối đã thành công. Kết nối bị đóng lại vì tôi chưa cấu hình mật khẩu cho Telnet, nhưng ACL vẫn hoạt động như mong đợi:



Bạn có thể thấy các gói tin đã khớp với access-list 3

**Cấu hình**

Cấu hình cuối cùng của từng thiết bị

**R1**

****

**R2**

****

Bây giờ bạn đã học được cách cấu hình Standard access-list và cách áp dụng cho các interfaces hoặc VTY line.