Danh sách truy cập trong chuẩn mạng TCP/IP

Bởi:

Ngô Bá Hùng, Phạm Thế Phi

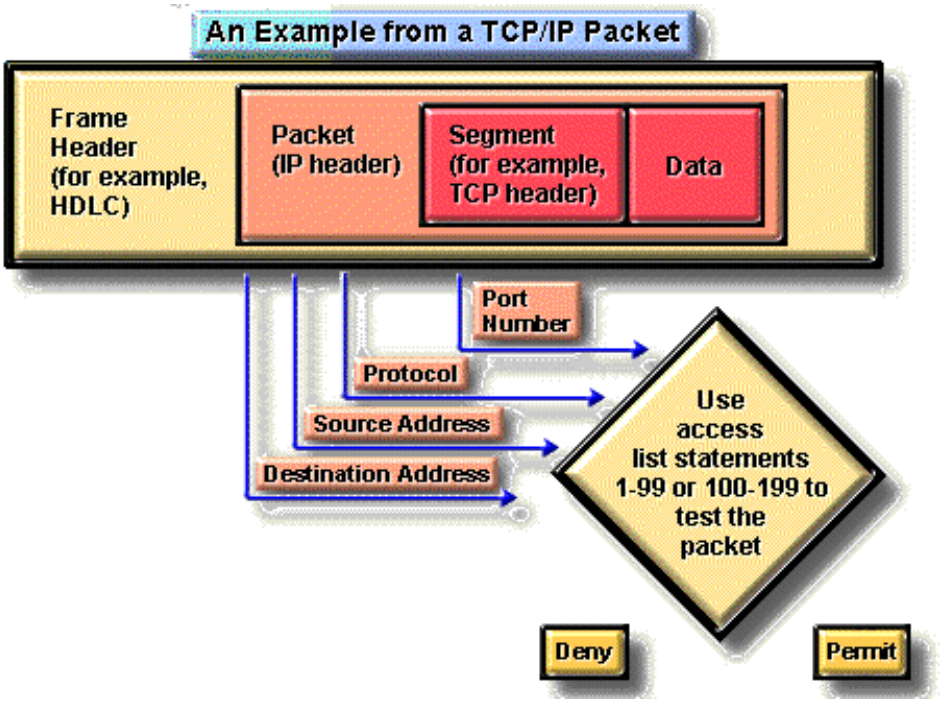
Danh sách truy cập trong chuẩn mạng TCP/IP

Kiểm tra các gói tin với danh sách truy cập

Để lọc các gói tin TCP/IP, danh sách truy cập trong hệ điều hành liên mạng của Cisco kiểm tra gói tin và phần tiêu đề của giao thức tầng trên.

Tiến trình này bao gồm các bước kiểm tra sau trên gói tin:

- Kiểm tra địa chỉ nguồn bằng danh sách truy cập chuẩn. Nhận dạng những danh sách truy cập này bằng các con số có giá trị từ 1 đến 99
- Kiểm tra địa chỉ đích và địa chỉ nguồn hoặc giao thức bằng danh sách truy cập mở rộng . Nhận dạng các danh sách này bằng các con số có giá trị từ 100 đến 199.
- Kiểm tra số hiệu cổng của các giao thức TCP hoặc UDP bằng các điều kiện trong các danh sách truy cập mở rộng. Các danh sách này cũng được nhận dạng bằng các con số có giá trị từ 100 đến 199.



Hình 7.5 – Ví dụ về danh sách truy cập trong gói tin TCP/IP

Đối với tất cả các danh sách truy cập của giao thức TCP/IP này, sau khi một gói tin được kiểm tra để khớp một lệnh trong danh sách, nó có thể bị từ chối hoặc cấp phép để sử dụng một giao diện trong nhóm các giao diện được truy cập.

Một số lưu ý khi thiết lập danh sách truy cập:

- Nhà quản trị mạng phải hết sức thận trọng khi đặc tả các điều khiển truy cập và thứ tự các lệnh để thực hiện các điều khiển truy cập này. Chỉ rõ các giao thức được phép trong khi các giao thức TCP/IP còn lại thì bị từ chối.
- Chỉ rõ các giao thức IP cần kiểm tra. Các giao thức IP còn lại thì không cần kiểm tra.
- Sử dụng các ký tự đại diện (wildcard) để mô tả luật chọn lọc địa chỉ IP.

Sử dụng các bit trong mặt nạ ký tự đại diện

Mặt nạ ký tự đại hiện (Wildcard mask) là một chuỗi 32 bits được dùng để kết hợp với địa chỉ IP để xác định xem bit nào trong địa chỉ IP được bỏ qua khi so sánh với các địa chỉ IP khác. Các mặt nạ ký tự đại diện này được mô tả khi xây dựng các danh sách truy cập. Ý nghĩa của các bits trong mặt nạ các ký tự đại diện được mô tả như sau:

- Một bits có giá trị là 0 trong mặt nạ đại diện có nghĩa là « hãy kiểm tra bit của địa chỉ IP có vị trí tương ứng với bit này »
- Một bits có giá trị là 1 trong mặt nạ đại diện có nghĩa là « đừng kiểm tra bit của địa chỉ IP có vị trí tương ứng với bit này »

Bằng cách thiết lập các mặt nạ ký tự đại diện, một nhà quản trị mạng có thể chọn lựa một hoặc nhiều địa chỉ IP để các kiểm tra cấp phép hoặc từ chối. Xem ví dụ trong hình dưới đây:

128	64	32	16	8	4	2	1	Vị trí các bit trong byte và giá trị địa chỉ của nó
0	0	0	0	0	0	0	0	Mặt nạ kiểm tra tất cả các bit địa chỉ
0	0	1	1	1	1	1	1	Mặt nạ không kiểm tra 6 bits cuối cùng của địa chỉ
0	0	0	0	1	1	1	1	Mặt nạ không kiểm tra 4 bits cuối cùng của địa chỉ
1	1	1	1	1	1	0	0	Mặt nạ kiểm tra 2 bits cuối cùng của địa chỉ
1	1	1	1	1	1	1	1	Mặt nạ không kiểm tra địa chỉ

Ví dụ: Cho một địa chỉ mạng ở lớp B 172.16.0.0. Mạng này được chia thành 256 mạng con bằng cách sử dụng 8 bit ở bytes thứ 3 của địa chỉ để làm số nhận dạng mạng con. Nhà quản trị muốn định kiểm tra các địa chỉ IP của các mạng con từ 172.16.16.0 đến 172.16.31. Các bước suy luận để đưa ra mặt nạ các ký tự đại diện trong trường hợp này như sau:

- Đầu tiên mặt nạ ký tự đại diện phải kiểm tra hai bytes đầu tiên của địa chỉ (172.16). Như vậy các bits trong hai bytes đầu tiên của mặt nạ ký tự đại diện phải bằng 0. Ta có 0000 0000.0000 0000.-.-
- Do không kiểm tra địa chỉ của các máy tính trong mạng nên các bit của bytes cuối cùng sẽ được bỏ qua. Vì thế các bits của bytes cuối cùng trong mặt nạ ký tự đại diện sẽ là 1. Ta có 0000 0000.0000 0000.-.1111 1111
- Trong byte thứ ba của địa chỉ nơi mạng con được định nghĩa, mặt nạ ký tự đại diện sẽ kiểm tra bit ở vị trí có giá trị thứ 16 của địa chỉ phải được bật (giá trị là 1) và các bits ở phần cao còn lại phải tắt (giá trị là 0). Vì thế các bits tương ứng trong mặt nạ ký tự đại diện phải bằng 0.
- Bốn bits còn lại của bytes thứ 3 không cần kiểm tra để nó có thể tạo nên các giá trị từ 16 đến 31. Vì thế các bits tương ứng trong mặt nạ ký tự đại diện tương ứng sẽ bằng 1.
- Như vậy mặt nạ ký tự đại diện là đầy đủ là: 0000 0000.0000 0000.0000 1111.1111 1111 hay 0.0.15.255

Để đơn giản, một số router, chẳng hạn CISCO, sử dụng một số từ viết tắt để chỉ một số mặt nạ thường sử dụng:

- any: dùng để chỉ mặt nạ cho phép tất cả địa chỉ (255.255.255.255) hoặc cấm tất cả (0.0.0.0.).

- host: được đặt phía trước một địa chỉ IP của một máy tính để chỉ rằng hãy kiểm tra tất cả các bit của địa chỉ trên. Ví dụ: host 172.16.1.1.

Cấu hình danh sách truy cập chuẩn cho giao thức IP

Phần này giới thiệu một số lệnh được hỗ trợ trong các router của Cisco.

Lệnh access list

Lệnh này dùng để tạo một mục từ trong danh sách bộ lọc chuẩn. Cú pháp như sau:

access-list *access-list-No {permit | deny } source {source-mask}*

Ý nghĩa của các tham số:

- access-list-No: Là số nhận dạng của danh sách truy cập, có giá trị từ 1 đến 99
- permit | deny: Tùy chọn cho phép hay không cho phép đối với giao thông của khối địa chỉ được mô tả phía sau.
- source: Là một địa chỉ IP
- source-mask: Là mặt nạ ký tự đại diện áp dụng lên khối địa chỉ source

Lệnh ip access-group

Lệnh này dùng để liên kết một danh sách truy cập đã tồn tại vào một giao diện. Cú pháp như sau:

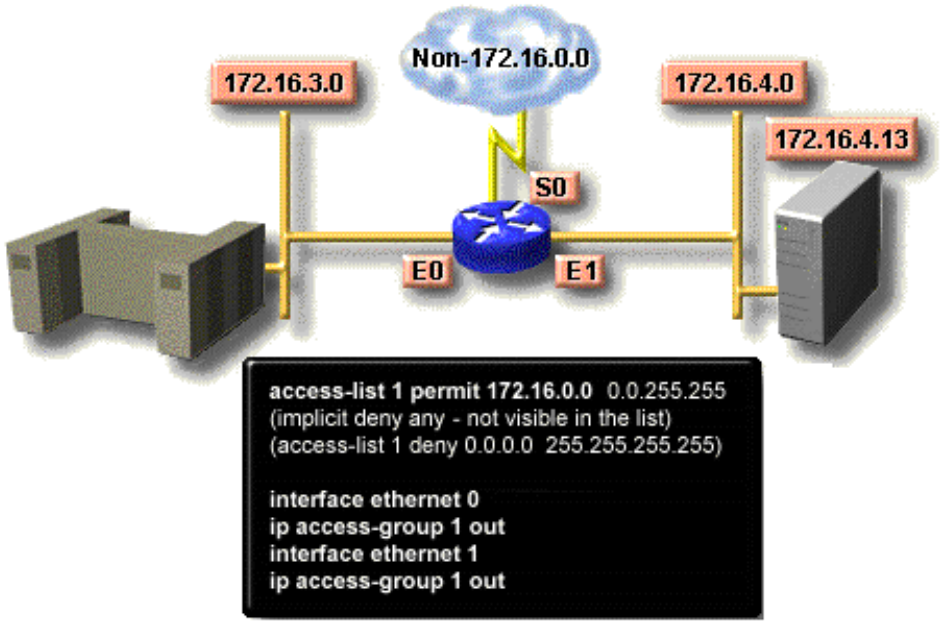
ip access-group *access-list-No {in/out}*

- access-list-no: số nhận dạng của danh sách truy cập được nối kết vào giao diện
- in/out: xác định chiều giao thông muốn áp dụng và vào hay ra.

Một số ví dụ

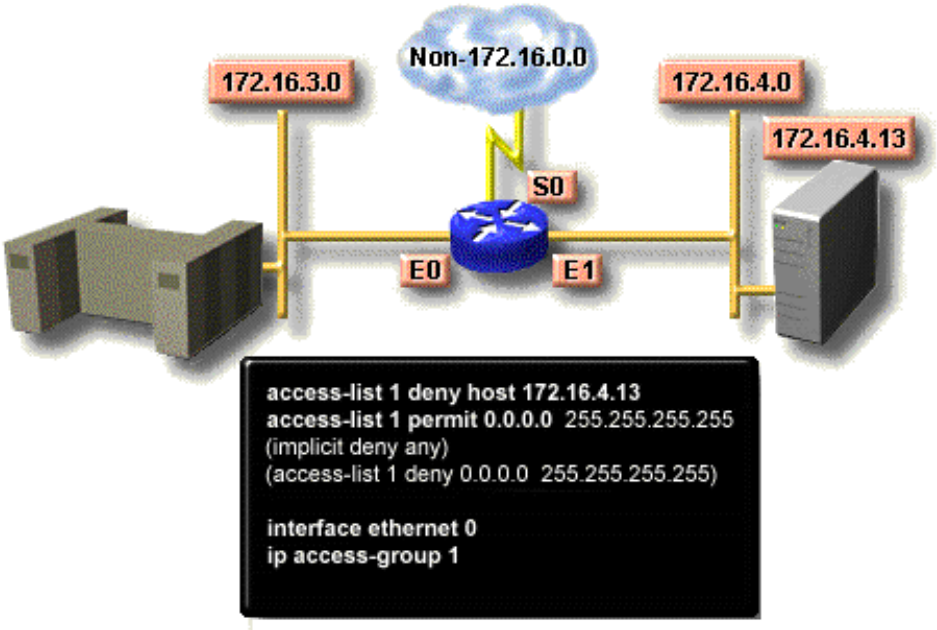
- Tạo danh sách truy cập chuẩn

Ví dụ 1



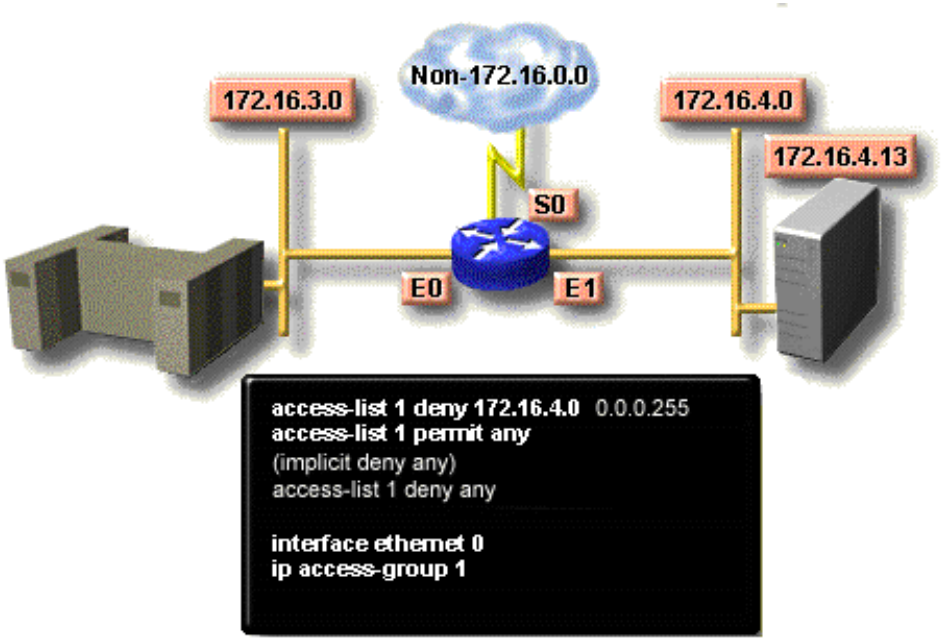
Danh sách truy cập trên chỉ cho phép các giao thông từ mạng nguồn 172.16.0.0 được chuyển tiếp đi qua router. Các giao thông trên các mạng khác đều bị khóa.

Ví dụ 2



Danh sách truy cập này được thiết kế để khóa các giao thông từ địa chỉ IP 172.16.1.13 và cho phép các luồng giao thông khác được chuyển tiếp qua các giao diện Ethernet (E0 và E1)

Ví dụ 3



Danh sách truy cập này được thiết kế để khóa luồng giao thông từ mạng con 172.16.4.0 và cho phép các luồng giao thông khác được chuyển tiếp.

Cấu hình danh sách truy cập mở rộng

Để có thể điều khiển việc lọc các luồng giao thông được chính xác hơn ta sử dụng các danh sách điều khiển truy cập mở rộng của giao thức IP. Các lệnh trong danh sách truy cập cho phép kiểm tra địa chỉ nguồn và địa chỉ nhận. Ngoài ra danh sách truy cập mở rộng còn cho phép đặc tả các cổng của các giao thức TCP và UDP. Các danh sách truy cập mở rộng thường sử dụng các số nhận dạng từ 100 đến 199. Phần kế tiếp sẽ mô tả các lệnh của danh sách truy cập mở rộng thường được hỗ trợ trong bởi các router .

Lệnh access-list

Lệnh này được sử dụng để tạo một mục từ để diễn giải một điều kiện lọc phức tạp. Cú pháp như sau:

access-list *access-list-no {permit|deny} protocol source source-mask*

destination destination-mask [operator operand] [established]

- *access-list-no:* Số nhận dạng của danh sách, có giá trị từ 100 đến 199
- *permit|deny:* chỉ định danh sách này dùng để cấp phép hay từ chối khối địa chỉ theo sau.

- *protocol:* có thể là một trong các giá trị sau IP, TCP, UDP, ICMP, GRE, IGRP.
- *source và destination:* Xác định địa chỉ IP gởi và nhận
- *source-mask và destination-mask:* là mặt nạ ký tự đại diện cho địa chỉ nguồn và địa chỉ đích.
- *operator và operand:* là một trong các phép toán sau lt, gt, eq, neq (nhỏ hơn, lớn hơn, bằng, không bằng), và một số hiệu cổng.
- *established*: Cho phép giao thức TCP duy trì nối kết

Lệnh ip access-group

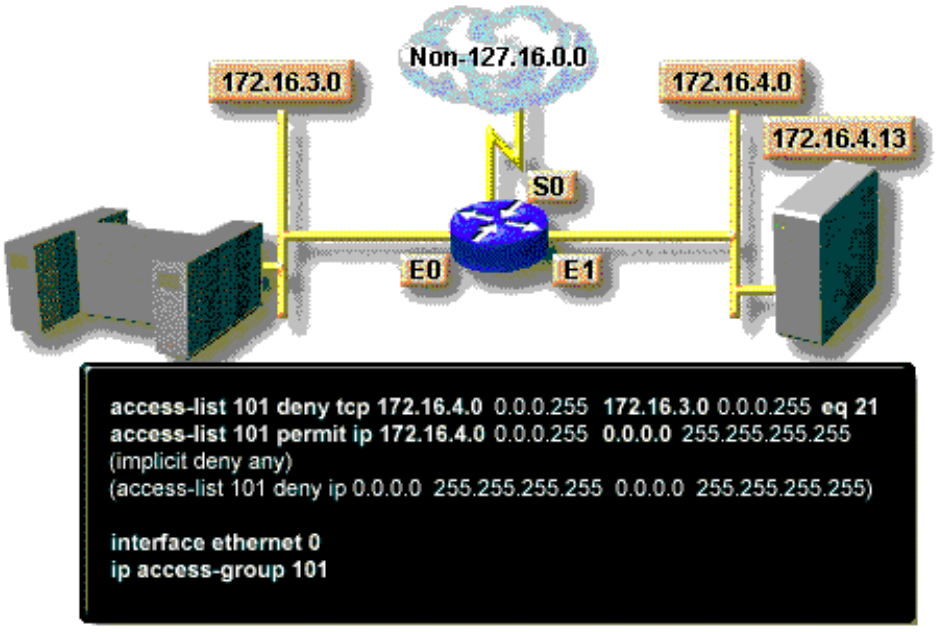
Nối kết một danh sách điều khiển nối kết mở rộng với một giao diện mạng ngỏ ra. Chỉ cho phép một danh sách điều khiển truy cập trên một cổng của một giao thức. Cú pháp như sau:

ip access-group *access-list-no {in|out}*

- access-list-no: là số nhận dạng của danh sách điều khiển truy cập mở rộng
- in|out: để xác định danh sách điều khiển truy cập này áo dụng cho giao diện vào hay ra.

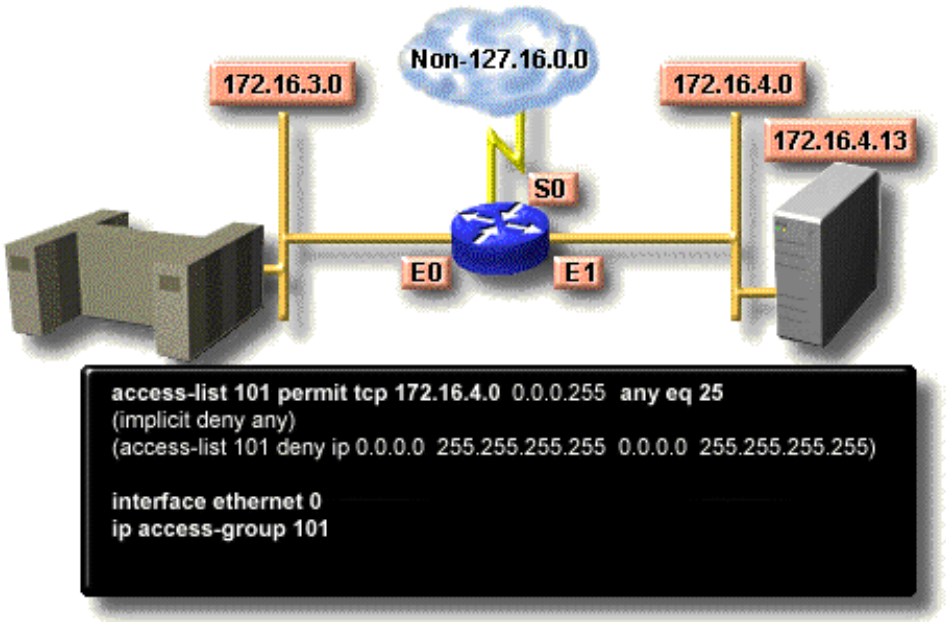
Một số ví dụ về danh sách điều khiển truy cập mở rộng

Ví dụ 1:



Danh sách điều khiển truy cập này được thiết kế để cho phép luồng giao thông từ mạng con 172.16.4.0 được chuyển đến bất kỳ một mạng hoặc mạng con khác thông qua giao diện E0.

Ví dụ 2:



Danh sách điều khiển truy cập này được thiết kế để chi cho phép thư điện tử từ mạng con 172.16.4.0 được gởi qua giao diện E0. Các luồng giao thông từ các mạng khác đều bị từ chối.

Nguyên tắc sử dụng danh sách điều khiển truy cập

Như vậy ta có hai loại danh sách điều khiển truy cập là danh sách điều khiển truy cập chuẩn và danh sách điều khiển truy cập mở rộng. Danh sách điều khiển truy cập chuẩn chỉ các gói tin dựa vào địa chỉ địa chỉ nguồn. Chính vì thế trong một mạng có nhiều router, nó cần được thiết lập ở router nằm gần thế giới bên ngoài nhất. Ngược lại, danh sách điều khiển truy cập mở rộng cho phép lọc dựa trên đích đến của các gói tin, vì thế chúng thường được đặt ở các router gần các máy nguồn nhất để ngăn chặn sớm các gói tin đến các đích đến không được phép.