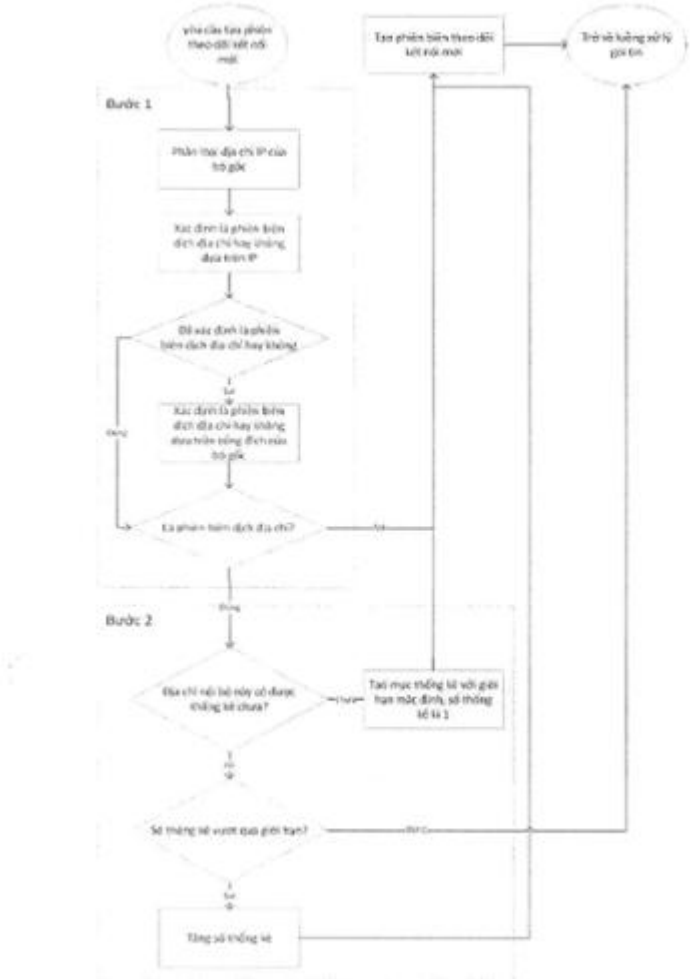
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0042149**
(51)[2020.01] **H04L 12/00**
(13) **B**

(21) 1-2020-05011
(22) 31/08/2020
(45) 25/12/2024 441
(43) 25/02/2021 395
(73) TẬP ĐOÀN CÔNG NGHIỆP - VIỄN THÔNG QUÂN ĐỘI (VN)
Lô D26 khu đô thị mới Cầu Giấy, phường Yên Hoà, quận Cầu Giấy, thành phố Hà Nội
(72) Trần Uy Hoàng (VN); Ngô Thị Minh Nguyệt (VN).
(74) Công ty TNHH Tư vấn Quốc Dân (NACILAW)

(54) PHƯƠNG PHÁP GIỚI HẠN SỐ PHIÊN BIÊN DỊCH ĐỊA CHỈ MẠNG CHO THIẾT BỊ TRONG MẠNG NỘI BỘ

(57) Sáng chế đề xuất phương pháp giới hạn số phiên biên dịch địa chỉ mạng cho thiết bị trong mạng nội bộ, thông qua việc theo dõi sự khởi tạo và hủy bỏ các phiên theo dõi bên trong khối xử lý mạng của hệ điều hành Linux, phân loại và thống kê các phiên theo dõi kết nối để có được dữ liệu thống kê các phiên biên dịch, từ đó giới hạn các phiên trên từng thiết bị dựa vào dữ liệu thống kê. Phương pháp bao gồm pha thiết lập và pha hoạt động.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề xuất phương pháp giới hạn số phiên biên dịch địa chỉ mạng cho thiết bị trong mạng nội bộ. Phương pháp giới hạn số phiên biên dịch địa chỉ mạng (phiên NAT) cho mỗi thiết bị mạng nội bộ của thiết bị định tuyến hộ gia đình, thông qua việc quản lý sự khởi tạo và hủy bỏ các phiên kết nối. Phương pháp được ứng dụng trên hệ điều hành Linux.

Tình trạng kỹ thuật của sáng chế

Hệ điều hành Linux hiện thực một cơ chế theo dõi các phiên kết nối gọi là "theo dõi kết nối" (connection tracking). Mỗi phiên theo dõi kết nối bao gồm các thông tin:

- Địa chỉ nguồn và đích của giao thức địa chỉ mạng (IP);
- Số hiệu cổng nguồn và đích tầng giao vận lớp 4 (transport protocol port number, gọi tắt là port) (nếu có);
- Giao thức: giao thức điều khiển truyền vận (Transmission control protocol – TCP) hay giao thức gói dữ liệu người dùng (User Datagram Protocol – UDP),…
- Một số thông tin khác như thời gian hết hạn,…

Mỗi phiên biên dịch địa chỉ của thiết bị trong mạng nội bộ ứng với một phiên theo dõi kết nối. Tuy nhiên một phiên theo dõi kết nối có thể ứng với một phiên biên dịch địa chỉ, hoặc một kết nối từ bản thân thiết bị đến thiết bị khác trong mạng nội bộ hoặc mạng diện rộng.

Số phiên theo dõi kết nối tồn tại cùng một lúc trong một thiết bị được giới hạn bởi bộ nhớ vật lý. Nếu số phiên theo dõi kết nối đạt đến giới hạn thì chỉ những gói tin thuộc các kết nối cũ được đi qua, không thể tạo kết nối mới cho đến khi một trong các phiên ứng với các kết nối cũ bị quá hạn (không có gói tin nào thuộc kết nối đó đi qua sau một thời gian nhất định, tùy vào trạng thái và giao thức). Lúc đó phiên theo dõi kết nối bị quá hạn sẽ bị xóa, nhường chỗ để tạo phiên mới.

Vấn đề xảy ra khi một thiết bị trong mạng nội bộ chịu một cuộc tấn công từ chối dịch vụ phân tán (Distributed Denial of Service – DDoS) khiến số phiên biên dịch địa chỉ kết nối đến thiết bị đó tăng cao, do đó các thiết bị khác không tạo được phiên kết nối mới. Một số trường hợp khác dẫn đến việc số phiên NAT kết nối đến một thiết bị trong mạng nội bộ tăng cao như sau:

- Người dùng cố ý hoặc vô ý (do mã độc,...) tạo hàng loạt phiên kết nối đến nhiều địa chỉ khác nhau nhằm mục đích phá hoại hạ tầng mạng.
- Người dùng sử dụng các phần mềm tải về phân luồng (ví dụ phần mềm BitTorrent) tạo nhiều phiên kết nối để tận dụng tối đa băng thông.

Trong hệ điều hành Linux, khối chịu trách nhiệm lọc các gói tin là "bộ lọc mạng" (netfilter) có khả năng giới hạn số gói tin gửi trong một đơn vị thời gian hoặc số kết nối mới trong một đơn vị thời gian. Điều này có thể giảm bớt hậu quả gây ra bởi những vấn đề nêu trên, tuy nhiên có thể gây giảm hiệu năng của mạng.

Xét ví dụ sau như hình 1:

- Thiết bị định tuyến hộ gia đình (gọi tắt là bộ định tuyến) có số phiên kết nối tối đa là 10000, thiết bị có khả năng tạo mới 100 phiên kết nối/giây.
- Một máy tính A trong mạng nội bộ bị nhiễm mã độc và tạo kết nối bằng gói tin đồng bộ của giao thức TCP.
- Thiết bị có cổng gi-ga-bít nên tốc độ rất cao, thiết bị định tuyến đạt tới giới hạn tạo 100 phiên kết nối/giây. Ở trạng thái đồng bộ, phiên kết nối TCP có thời gian quá hạn là 120 giây. Sau khoảng 10000/100 = 100 giây, bộ định tuyến đạt số phiên kết nối tối đa, các thiết bị trong mạng nội bộ không thể tạo được kết nối mới cho đến 20 giây sau, khi những phiên kết nối đầu tiên tạo bởi máy tính A bị quá hạn.
- Để cô lập cuộc tấn công này khi nó xảy ra lần sau, bộ lọc mạng được thiết lập để cho phép máy tính A tạo được tối đa 50 phiên kết nối/giây. Như vậy, lần sau khi máy A bị tấn công, sau 100 giây, nó tạo được 5000 phiên kết nối, sau 120 giây, nó tạo được 6000 phiên kết nối, không đủ để làm quá tải bộ định tuyến, các thiết bị khác trong mạng nội bộ vẫn có thể tạo phiên kết nối mới. Như vậy, cách hiện thực này chống được cuộc tấn công.

- Tiếp tục xét ví dụ trên, vì là một thiết bị hiệu suất cao nên đôi lúc máy A lại cần tạo lên đến 100 phiên kết nối/giây. Tuy nhiên do bị giới hạn, máy A chỉ tạo được 50 phiên kết nối đầu tiên. Đối với 50 phiên kết nối còn lại, gói tin mào đầu phiên kết nối bị chặn ở bộ định tuyến. Máy A chỉ biết được việc này sau 120 giây không thấy phản hồi cho các gói mào đầu của 50 phiên kết nối sau. Lúc này nó mới gửi lại 50 gói tin mào đầu. Thay vì mất 1 giây để tạo 100 phiên, thì máy A phải mất 121 giây để tạo được 100 phiên.

Như vậy, cần có một cách hiện thực khác để giảm số phiên kết nối qua bộ định tuyến, làm sao cho vừa đảm bảo hiệu năng, vừa phòng chống các cuộc tấn công hiệu quả.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là giới hạn số phiên biên dịch địa chỉ mạng cho thiết bị trong mạng nội bộ của thiết bị định tuyến hộ gia đình. Để đạt được mục đích trên, sáng chế được đề xuất bao gồm 2 pha:

Pha 1: pha thiết lập; tại pha này, tiến hành thiết lập giới hạn cho từng thiết bị trong mạng nội bộ.

Các thiết bị trong mạng nội bộ được đặc trưng bởi địa chỉ IP. Sáng chế yêu cầu có thể thiết lập giá trị giới hạn mặc định và giá trị giới hạn riêng, giới hạn số phiên biên dịch địa chỉ trên từng thiết bị.

Pha 2: pha hoạt động; tại pha này, tiến hành theo dõi các việc khởi tạo và xóa các phiên theo dõi kết nối. Thực hiện các bước sau mỗi khi khởi tạo và xóa các phiên:

Bước 1: loại trừ các phiên theo dõi kết nối không phải là phiên biên dịch địa chỉ.

Bước 2: thay đổi giá trị thống kê.

Mô tả vắn tắt các hình vẽ

Hình 1 là hình vẽ mô tả cấu trúc mạng phổ biến của thiết bị định tuyến hộ gia đình trong chức năng biên dịch địa chỉ.

Hình 2 là hình vẽ mô tả luồng xử lý các gói tin với khối bộ lọc mạng trong nhân của hệ điều hành Linux;

Hình 3 là sơ đồ mô tả luồng theo dõi khi phiên theo dõi kết nối mới được tạo;

Hình 4 là sơ đồ mô tả luồng theo dõi khi xóa một phiên theo dõi kết nối.

Mô tả chi tiết sáng chế

Biên dịch địa chỉ mạng (tiếng Anh là Network address translation – NAT) là quá trình thay đổi thông tin địa chỉ IP trong gói tin được truyền qua thiết bị định tuyến. Trong nhiều dịch vụ mạng cho hộ gia đình, biên dịch địa chỉ mạng là cần thiết để nhiều thiết bị khác nhau có thể sử dụng dịch vụ cùng lúc với một địa chỉ mạng công cộng duy nhất.

Biên dịch địa chỉ mạng được thực hiện trong nhân hệ điều hành Linux qua khối bộ lọc mạng. Hình 2 thể hiện luồng xử lý gói tin với khối bộ lọc mạng. Gói tin được bộ lọc mạng xử lý tại 5 vị trí (hook):

- Tiền định tuyến (PREROUTING): Khi gói tin đi vào khối xử lý mạng, trước khi quá trình định tuyến xảy ra;
- Ngõ vào (INPUT): Sau khi quyết định gói tin dành cho chính thiết bị, chuẩn bị đưa vào xử lý nội bộ;
- Chuyển tiếp (FORWARD): Sau khi quyết định gói tin dành cho thiết bị khác;
- Ngõ ra (OUTPUT): Gói tin đi ra từ thiết bị, sau quá trình xử lý nội bộ;
- Hậu định tuyến (POSTROUTING): Trước khi đi ra giao diện mạng.

Bảng IP (iptables) là giao diện người dùng để cấu hình khối bộ lọc mạng. Bảng IP gồm nhiều bảng con, mỗi bảng con thực hiện một nhiệm vụ:

- Bộ lọc (filter): thực hiện lọc các gói tin;
- Biên dịch địa chỉ (nat): thực hiện thay đổi các địa chỉ mạng ở lớp 3, lớp 4;
- Xé (mangle): thực hiện các thao tác thay đổi tiêu đề của gói tin.
- Thô (raw): thực hiện các thao tác xử lý gói tin trước khi cơ chế theo dõi kết nối (connection tracking) hoạt động.

Biên dịch địa chỉ mạng được hiện thực với bảng biên dịch địa chỉ (nat) của bảng IP, bằng cách thêm một luật hậu định tuyến, thay đổi địa chỉ nguồn của gói

tin từ địa chỉ IP của máy trong mạng nội bộ thành địa chỉ IP giao diện mạng diện rộng của thiết bị định tuyến hộ gia đình. Thao tác này còn gọi là giả dạng IP (IP Masquerade).

Xét cấu trúc mạng được ví dụ như hình 1, một ứng dụng ở máy A muốn tạo một kết nối TCP đến máy chủ ở 22.22.22.22. Khi gói tin đầu tiên của kết nối đi từ mạng nội bộ vào thiết bị định tuyến hộ gia đình, đến vị trí tiền định tuyến trong khối xử lý mạng, nó sẽ tạo một phiên theo dõi kết nối mới. Mỗi phiên gồm 2 bộ (tuple), bộ gốc và bộ trả lời. Mỗi bộ chứa thông tin bao gồm địa chỉ IP nguồn, số hiệu nguồn, địa chỉ IP đích, số hiệu đích, giao thức,... của các gói tin theo một hướng của kết nối. Thông tin của phiên theo dõi kết nối được thể hiện ở bảng dưới:

	IP nguồn	Số hiệu nguồn	IP đích	Số hiệu đích	Giao thức
Bộ gốc	192.168.1.2	50000	22.22.22.22	80	TCP
Bộ trả lời	22.22.22.22	80	192.168.1.2	50000	TCP

Trong quá trình xử lý trong khối xử lý mạng, gói tin đi đến vị trí hậu định tuyến và được tiến hành thao tác biên dịch địa chỉ. Đổi địa chỉ IP nguồn của gói tin từ 192.168.1.2 thành 11.11.11.11. Đồng thời, thay đổi bộ trả lời của phiên theo dõi kết nối vừa tạo thành như bảng:

	IP nguồn	Số hiệu nguồn	IP đích	Số hiệu đích	Giao thức
Bộ gốc	192.168.1.2	50000	22.22.22.22	80	TCP
Bộ trả lời	22.22.22.22	80	11.11.11.11	50000	TCP

Như vậy, gói tin trả về từ máy chủ có địa chỉ đích 11.11.11.11 sẽ được tra cứu xem có thuộc các phiên theo dõi kết nối hiện tại hay không. Nếu thuộc một phiên hiện tại, nó sẽ được thay đổi địa chỉ IP đích và đi đến máy tính trong mạng nội bộ theo đường cũ, dựa trên thông tin của phiên theo dõi kết nối đã được lưu.

Ngoài việc được dùng như là các phiên biên dịch địa chỉ, theo dõi kết nối còn được dùng cho các gói tin đi vào hoặc đi ra từ chính thiết bị định tuyến. Vì vậy cần phân loại các phiên theo dõi kết nối trước khi dùng cho mục đích theo dõi các phiên biên dịch địa chỉ.

Phương pháp giới hạn các phiên biên dịch địa chỉ cho mạng nội bộ trong thiết bị định tuyến hộ gia đình được thực hiện gồm 2 pha:

Pha 1: pha thiết lập; tại pha này, tiến hành thiết lập giới hạn cho từng thiết bị trong mạng nội bộ.

Các thiết bị trong mạng nội bộ như máy tính để bàn, máy tính xách tay, điện thoại thông minh,... được đặc trưng bởi địa chỉ IP. Sáng chế yêu cầu có thể thiết lập giá trị giới hạn mặc định và giá trị giới hạn riêng, giới hạn số phiên biên dịch địa chỉ trên từng thiết bị. Nếu một thiết bị (ứng với một địa chỉ IP) được thiết lập giới hạn riêng thì số phiên biên dịch địa chỉ tối đa mà bộ định tuyến cấp phát cho thiết bị đó chính bằng giới hạn riêng được thiết lập. Nếu thiết bị không được thiết lập giới hạn riêng thì số phiên biên dịch địa chỉ tối đa đối với thiết bị đó bằng giá trị giới hạn mặc định. Các giá trị giới hạn này được thiết lập dựa trên khả năng của thiết bị định tuyến (bộ định tuyến có khả năng xử lý tối đa bao nhiêu phiên tại một thời điểm) và nhu cầu thực tế của các thiết bị trong mạng.

Pha 2: pha hoạt động; tại pha này, tiến hành theo dõi các việc khởi tạo và xóa các phiên theo dõi kết nối. Như được thể hiện trên hình 3 và hình 4, các bước để khởi tạo và xóa các phiên theo dõi kết nối mới bao gồm:

Bước 1: loại trừ các phiên theo dõi kết nối không phải là phiên biên dịch địa chỉ.

Để nhận diện các phiên không phải phiên biên dịch địa chỉ, cần phân loại địa chỉ IP nguồn và đích của bộ gốc bằng cách so sánh các địa chỉ đó qua mặt nạ mạng con:

- Địa chỉ vòng lại: nếu địa chỉ trùng dải mạng 127.0.0.0/8 thì là địa chỉ vòng lại.
- Địa chỉ đa bá (multicast): nếu địa chỉ nằm trong dải từ 224.0.0.0 đến 239.255.255.255.

- Địa chỉ quảng bá (broadcast): nếu địa chỉ là địa chỉ lớn nhất trong dải mạng của một giao diện trong bộ định tuyến.
- Địa chỉ của bộ định tuyến: nếu địa chỉ IP trùng khớp với bất kì giao diện nào của bộ định tuyến.
- Địa chỉ của máy trong mạng nội bộ: nếu địa chỉ IP trùng với dải mạng giao diện mạng nội bộ.
- Địa chỉ mạng diện rộng: bao gồm các địa chỉ còn lại.

Nếu bộ gốc không bao gồm địa chỉ vòng lại thì ta tiếp tục phân loại phiên theo dõi địa chỉ dựa trên loại địa chỉ IP nguồn và đích của bộ gốc như bảng dưới:

STT	IP nguồn của bộ gốc	IP đích của bộ gốc	Ghi chú	Là phiên biên dịch địa chỉ
1	Địa chỉ của bộ định tuyến	Địa chỉ của máy trong mạng nội bộ, địa chỉ đa bá, địa chỉ quảng bá, địa chỉ mạng diện rộng	Kết nối xuất phát từ bộ định tuyến	Sai
2	Địa chỉ của máy trong mạng nội bộ	Địa chỉ của bộ định tuyến	Kết nối từ mạng nội bộ đến bộ định tuyến	Sai
3	Địa chỉ của máy trong mạng nội bộ	Địa chỉ quảng bá	Quảng bá mạng nội bộ	Sai
4	Địa chỉ của máy trong mạng nội bộ	Địa chỉ mạng diện rộng, địa chỉ đa bá	Kết nối từ mạng nội bộ đến mạng diện rộng	Đúng
5	Địa chỉ mạng diện rộng	Địa chỉ của bộ định tuyến	- Kết nối từ mạng diện rộng đến máy	Đúng với trường hợp kết

			trong mạng nội bộ thông qua vùng phi quân sự (DMZ) hoặc chuyển tiếp cổng (port forwarding). - Kết nối từ mạng diện rộng đến bộ định tuyến	nối đến mạng nội bộ, sai với trường hợp kết nối đến bộ định tuyến

Các tổ hợp địa chỉ IP nguồn và đích không được liệt kê trong bảng trên không tồn tại nếu các thiết bị trong mạng hoạt động đúng chức năng. Nếu có lỗi từ thiết bị khác khiến địa chỉ nguồn và đích rơi vào các trường hợp không được liệt kê, thì bộ định tuyến cũng xem như đó không phải là phiên biên dịch địa chỉ.

Sau khi phân loại phiên dựa vào các địa chỉ IP, nếu đã xác định được đó là phiên biên dịch địa chỉ (trường hợp 4) thì tiếp tục đến bước 2 – thay đổi giá trị thống kê. Nếu xác định không phải là phiên biên dịch địa chỉ (trường hợp 1,2,3, trường hợp bộ gốc có địa chỉ vòng lại hoặc các trường hợp không được liệt kê) thì quay về luồng xử lý gói tin của nhân, tạo phiên theo dõi kết nối mới bình thường, không xét thống kê phiên này.

Với trường hợp 5, vẫn chưa xác định được đó là phiên biên dịch địa chỉ hay không thì cần xét đến các cổng đích (port TCP hoặc UDP) của bộ gốc. Trên giao diện mạng diện rộng, bộ định tuyến chỉ lắng nghe một số cổng, phục vụ cho quá trình quản lý và điều khiển bộ định tuyến từ phía nhà mạng. Vì vậy, nếu cổng đích của bộ gốc nằm trong danh sách các cổng quản lý và điều khiển nói trên thì phiên theo dõi kết nối chứa bộ gốc đó là một phiên kết nối đến bộ định tuyến, không phải phiên biên dịch địa chỉ. Trường hợp cổng đích của bộ gốc không thuộc các cổng mà bộ định tuyến đang lắng nghe thì có thể xem đó là phiên biên dịch địa chỉ cho các chức năng như vùng phi quân sự (DMZ) hoặc chuyển tiếp cổng (port

forwarding). Bộ định tuyến tiếp tục chuyển đến bước thay đổi giá trị thống kê đối với các phiên biên dịch địa chỉ hoặc quay về luồng xử lý gói tin của nhân đối với các phiên khác.

Bước 2: thay đổi giá trị thống kê. Dựa theo địa chỉ IP của máy trong mạng nội bộ vừa xác định ở trên, xét trong hai trường hợp:

- Trường hợp khởi tạo các phiên theo dõi kết nối, tiến hành tăng số liệu thống kê và thực hiện các hành động cần thiết khác:

  Tăng số liệu thống kê số phiên biên dịch địa chỉ của IP thêm 1 đơn vị.

  Nếu số liệu thống kê vượt quá giới hạn riêng của IP tương ứng, quay về luồng xử lý gói tin của nhân và không cho phép tạo phiên theo dõi kết nối mới. Gói tin mào đầu cho phiên theo dõi kết nối cũng bị hủy.

- Trường hợp xóa các phiên theo dõi kết nối, tiến hành giảm số liệu thống kê đi một đơn vị và thực hiện các hành động nếu cần:

  Nếu số liệu thống kê lớn hơn 0 thì giảm số liệu thống kê số phiên biên dịch địa chỉ của IP đi 1 đơn vị.

  Nếu số liệu thống kê nhỏ hơn hoặc bằng 0 thì không làm thay đổi giá trị thống kê.

  Tiếp theo là quay về luồng xử lý gói tin của nhân và tiếp tục hủy phiên theo dõi kết nối như bình thường.

Ví dụ thực hiện sáng chế

Cấu trúc mạng của ví dụ về phương pháp giới hạn số phiên biên dịch địa chỉ của từng thiết bị trong mạng nội bộ của thiết bị định tuyến hộ gia đình được thể hiện ở hình 1.

Trong ví dụ, mạng nội bộ của bộ định tuyến bao gồm 2 thiết bị là máy A và máy B. Hai máy này hoạt động đồng thời và tạo các kết nối đến các máy chủ trong mạng WAN. Số phiên biên dịch địa tối đa trong một lúc của bộ định tuyến là 10000. Máy A được giới hạn số phiên biên dịch địa chỉ mạng là 4000, giới hạn đối với máy B là 7000.

Giả sử ở một thời điểm, bộ định tuyến đang giữ 4000 phiên biên dịch địa chỉ cho máy A, 4000 phiên biên dịch địa chỉ cho máy B.

- Máy A mong muốn tạo một kết nối mới đến máy chủ 22.22.22.22:
    + Gói tin đầu tiên của kết nối là gói tin TCP có địa chỉ IP nguồn 192.168.1.2, số hiệu nguồn 50000, địa chỉ IP đích 22.22.22.22, số hiệu đích 80 được gửi vào bộ định tuyến.
    + Tại vị trí tiền định tuyến, cơ chế theo dõi kết nối của nhân hệ điều hành Linux trong bộ định tuyến hoạt động.
    + Phát hiện gói tin vừa được gửi không thuộc phiên theo dõi kết nối nào, hệ điều hành quyết định tạo phiên mới với bộ gốc có thông tin giống như gói tin vừa nhận, bộ trả lời có các thông tin địa chỉ/cổng nguồn và đích ngược lại với bộ gốc.
    + Khi cấp phát bộ nhớ cho phiên theo dõi kết nối mới, hệ điều hành thực hiện các bước thông kê để giới hạn số phiên biên dịch địa chỉ.

        Bước đầu tiên, hệ điều hành kiểm tra được gói tin không dành cho bộ định tuyến, không xuất phát từ bộ định tuyến cũng như không phải của kết nối nội bộ.

        Bước tiếp theo nhận diện được địa chỉ gốc của phiên theo dõi kết nối là 192.168.1.2.

        Đến bước thông kê, nhận thấy địa chỉ 192.168.1.2 đã tạo 4000 phiên kết nối và đạt đến giới hạn, hệ điều hành quyết định không tạo phiên theo dõi kết nối mới. Gói tin bị hủy và không được tiếp tục xử lý.
- Cùng lúc đó, máy B tạo một kết nối mới đến máy chủ 44.44.44.44:
    + Gói tin đầu tiên của kết nối là gói tin UDP có địa chỉ IP nguồn 192.168.1.3, số hiệu nguồn 50001, địa chỉ IP đích 44.44.44.44, số hiệu đích 53 đi vào bộ định tuyến.
    + Tại điểm tiền định tuyến, gói tin kích hoạt cơ chế theo dõi kết nối.

+ Sau các bước kiểm tra là phiên NAT hợp lệ, phiên theo dõi kết nối mới được tạo với thống kê số phiên NAT của IP 192.168.1.3 được tăng lên thành 4001 (số liệu thống kê vẫn chưa đạt đến giới hạn là 7000). Phiên theo dõi kết nối mới có bộ gốc với thông tin giống như gói tin vừa nhận và bộ trả lời với các thông tin địa chỉ/cổng nguồn và đích ngược lại với bộ gốc.

+ Gói tin UDP đi tiếp đến các điểm chuyển tiếp và hậu định tuyến. Tại điểm hậu định tuyến, nó được biên dịch địa chỉ nguồn thành 11.11.11.11, số hiệu nguồn 51001, đồng thời bộ trả lời của phiên theo dõi kết nối vừa được tạo cũng được thay đổi thành: IP nguồn 44.44.44.44, số hiệu nguồn 53, IP đích 11.11.11.11, số hiệu đích 51001.

+ Sau này, gói tin có thông tin địa chỉ giống với bộ gốc hoặc bộ trả lời sẽ không kích hoạt tạo phiên theo dõi kết nối mới, cho đến khi phiên bị quá hạn và bị xóa.

Sau một thời gian, một phiên theo dõi kết nối của IP 192.168.1.2 bị quá hạn, hệ điều hành quyết định xóa phiên đó. Trong lúc xóa phiên, hệ điều hành cũng kiểm tra phiên theo dõi kết nối có ứng với phiên biên dịch địa chỉ nào không. Tiếp theo đó là giảm thông số thông kê số phiên của IP 192.168.1.2. Số phiên lúc này nhỏ hơn 4000, máy A lại có thể tiếp tục tạo kết nối mới.

Hiệu quả đạt được của sáng chế

Phương pháp giới hạn số phiên biên dịch địa chỉ mạng cho thiết bị trong mạng nội bộ có thể giúp cô lập các cuộc tấn công DDoS hoặc tấn công phá hoại hạ tầng mạng vào phạm vi thiết bị, không ảnh hưởng lớn đến các thiết bị khác. Phương pháp này cũng có thể đảm bảo cân bằng các thiết bị trong mạng, không một thiết bị nào có thể dùng quá nhiều phiên kết nối; đồng thời có thể kết hợp với các biện pháp giới hạn băng thông theo phiên kết nối để giới hạn băng thông của thiết bị, đảm bảo chất lượng dịch vụ đồng đều giữa các máy.

Yêu cầu bảo hộ

1. Phương pháp giới hạn các phiên biên dịch địa chỉ cho mạng nội bộ trong thiết bị định tuyến hộ gia đình được thực hiện gồm 2 pha:

pha 1: pha thiết lập; tại pha này, tiến hành thiết lập giới hạn cho từng thiết bị trong mạng nội bộ;

các thiết bị trong mạng nội bộ được đặc trưng bởi địa chỉ IP; sáng chế yêu cầu có thể thiết lập giới hạn số phiên biên dịch địa chỉ chung cho từng thiết bị và/hoặc thiết lập giới hạn riêng cho từng thiết bị;

pha 2: pha hoạt động; tại pha này, tiến hành theo dõi các việc khởi tạo và xóa các phiên theo dõi kết nối; các bước để khởi tạo và xóa các phiên theo dõi kết nối mới bao gồm:

bước 1: loại trừ các phiên theo dõi kết nối không phải là phiên biên dịch địa chỉ;

để nhận diện các phiên không phải phiên biên dịch địa chỉ, cần phân loại địa chỉ IP nguồn và đích của bộ gốc bằng cách so sánh các địa chỉ đó qua mặt nạ mạng con:

địa chỉ vòng lại: nếu địa chỉ trùng dải mạng 127.0.0.0/8 thì là địa chỉ vòng lại;

địa chỉ đa bá: nếu địa chỉ nằm trong dải từ 224.0.0.0 đến 239.255.255.255;

địa chỉ quảng bá: nếu địa chỉ là địa chỉ lớn nhất trong dải mạng của một giao diện trong bộ định tuyến;

địa chỉ của bộ định tuyến: nếu địa chỉ IP trùng khớp với bất kì giao diện nào của bộ định tuyến

địa chỉ của máy trong mạng nội bộ: nếu địa chỉ IP trùng với dải mạng giao diện mạng nội bộ;

địa chỉ mạng diện rộng: bao gồm các địa chỉ còn lại;

nếu bộ gốc không bao gồm địa chỉ vòng lại thì ta tiếp tục phân loại phiên theo dõi địa chỉ dựa trên loại địa chỉ IP nguồn và đích của bộ gốc; bước 2: thay

đổi giá trị thống kê; dựa theo địa chỉ IP của máy trong mạng nội bộ vừa xác định ở trên, xét trong hai trường hợp:

trường hợp khởi tạo các phiên theo dõi kết nối, tiến hành tăng số liệu thống kê và thực hiện các hành động cần thiết khác:

tăng số liệu thống kê số phiên biên dịch địa chỉ của IP thêm 1 đơn vị;

nếu số liệu thống kê vượt quá giới hạn riêng của IP tương ứng, quay về luồng xử lý gói tin của nhân và không cho phép tạo phiên theo dõi kết nối mới; gói tin mào đầu cho phiên theo dõi kết nối cũng bị hủy;

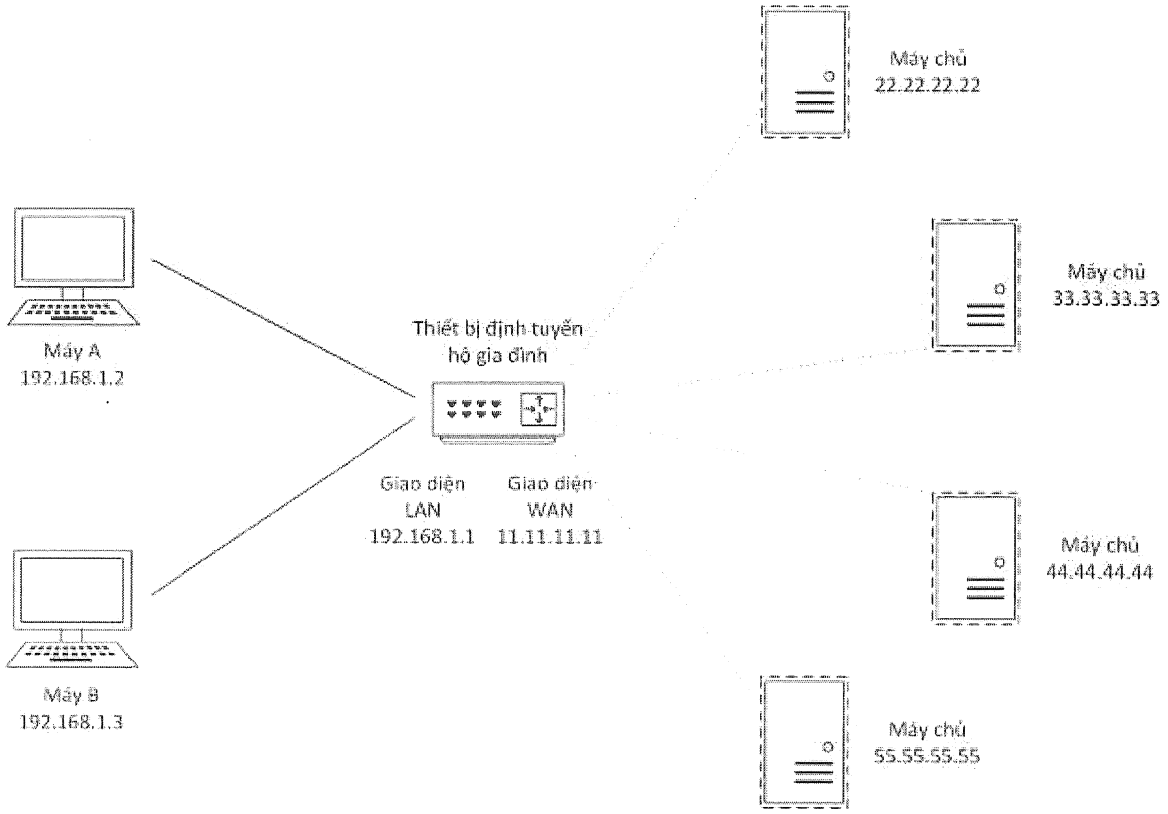
trường hợp xóa các phiên theo dõi kết nối, tiến hành giảm số liệu thống kê đi một đơn vị và thực hiện các hành động nếu cần:

nếu số liệu thống kê lớn hơn 0 thì giảm số liệu thống kê số phiên biên dịch địa chỉ của IP đi 1 đơn vị;

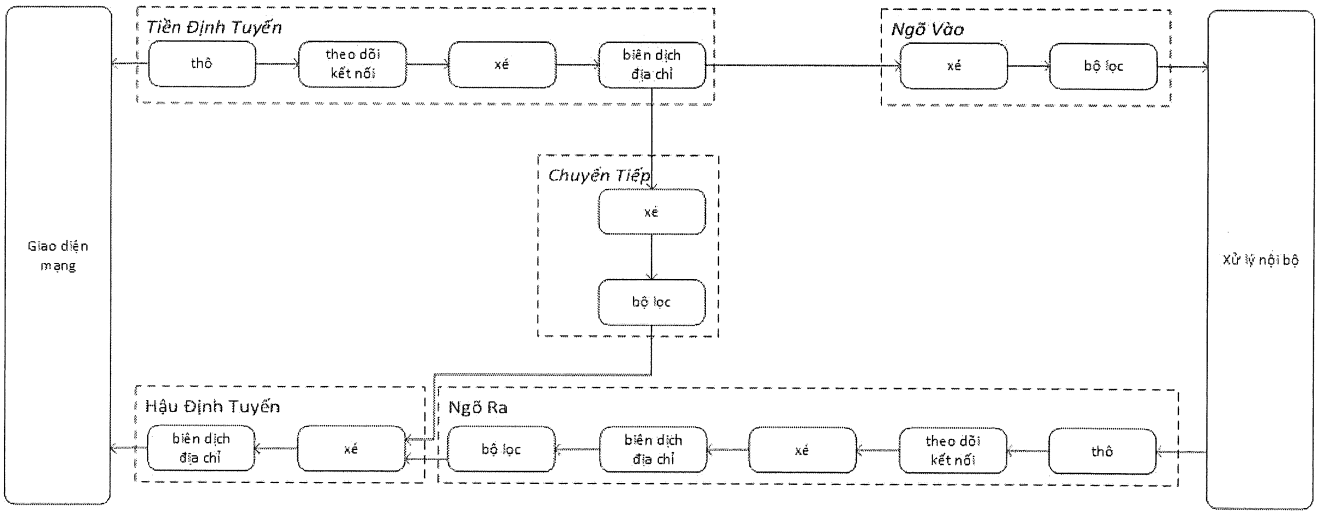
nếu số liệu thống kê nhỏ hơn hoặc bằng 0 thì không làm thay đổi giá trị thống kê;

tiếp theo là quay về luồng xử lý gói tin của nhân và tiếp tục hủy phiên theo dõi kết nối như bình thường.

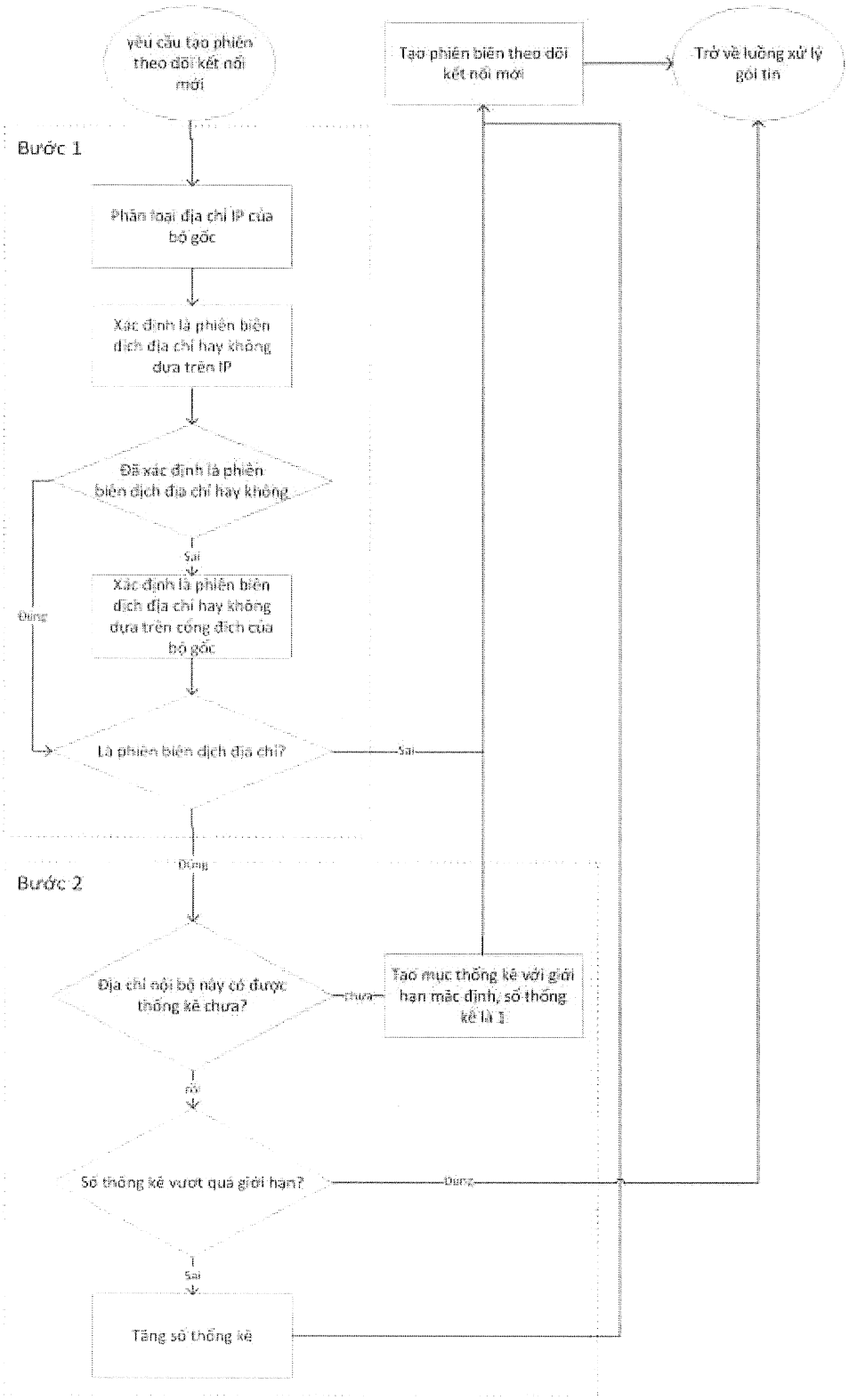
Hình vẽ



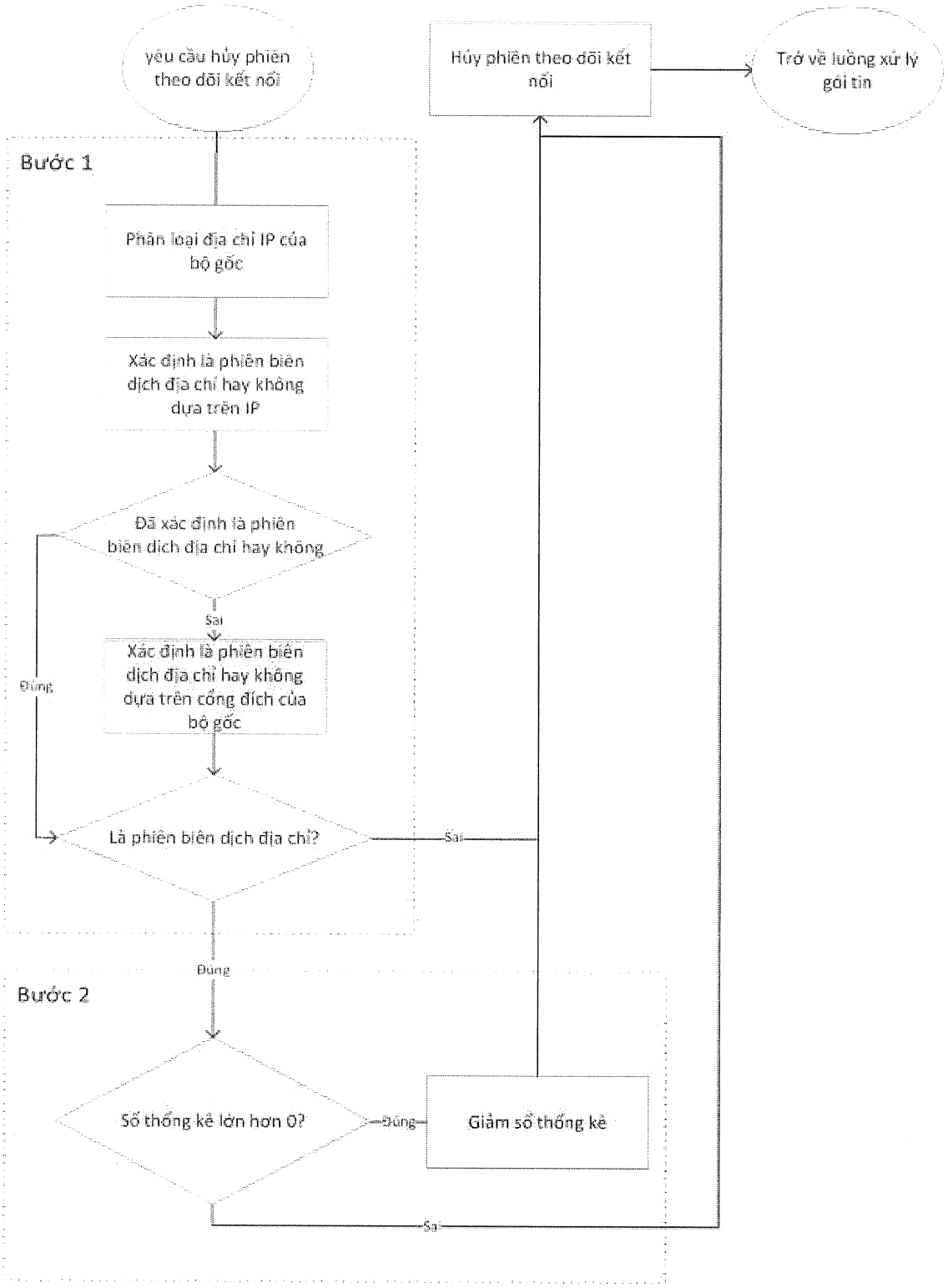
Hình 1



Hình 2


yêu cầu tạo phiên theo dõi kết nối mới
Tạo phiên biên theo dõi kết nối mới
Trở về luồng xử lý gói tin
Bước 1
Phân loại địa chỉ IP của bộ gốc
Xác định là phiên biên dịch địa chỉ hay không dựa trên IP
Đã xác định là phiên biên dịch địa chỉ hay không
Sai
Xác định là phiên biên dịch địa chỉ hay không dựa trên cổng đích của bộ gốc
Đúng
Là phiên biên dịch địa chỉ?
Sai
Đúng
Bước 2
Địa chỉ nội bộ này có được thống kê chưa?
Chưa
Tạo mục thống kê với giới hạn mặc định, số thống kê là 1
Rồi
Số thống kê vượt quá giới hạn?
Đúng
Sai
Tăng số thống kê

Hình 3


yêu cầu hủy phiên theo dõi kết nối
Hủy phiên theo dõi kết nối
Trở về luồng xử lý gói tin
Bước 1
Phân loại địa chỉ IP của bộ gốc
Xác định là phiên biên dịch địa chỉ hay không dựa trên IP
Đã xác định là phiên biên dịch địa chỉ hay không
Sai
Xác định là phiên biên dịch địa chỉ hay không dựa trên cổng đích của bộ gốc
Đúng
Là phiên biên dịch địa chỉ?
Sai
Đúng
Bước 2
Số thống kê lớn hơn 0?
Đúng
Giảm số thống kê
Sai

Hình 4