<https://github.com/trimstray/iptables-essentials>

[BELL94] Steven M. Bellovin and William R. Cheswick – network firewall. Ieee communications magazine 1994

Network firewall

Bảo mật máy tính là một vấn đề khó. Bảo mật máy tính được kết nối mạng còn khó hơn nhiều. Tường lửa (rào cản giữa 2 mạng) khi được sử dụng đúng cách sẽ gia tăng đáng kể sự bảo mật của máy tính.

Một Adminsistrator với một host có thể

William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin-Firewalls and Internet Security\_ Repelling the Wily Hacker-Addison-Wesley Professional

Security policy:

Chính sách bảo mật là tập hợp các quyết định chung, xác định tư thế của tổ chức về an ninh. Chính xác hơn, chính sách bảo mật phân định ranh giới của hành vi có thể chấp nhận được và phản ứng đối với các vi phạm như thế nào. Đương nhiên, các chính sách bảo mật sẽ khác nhau giữa tổ chức và tổ chức. Một trường học có nhu cầu khác với một tổ chức phát triển sản phẩm của công ty, mà cũng khác với một trang web quân sự.

Để xác định được các chính sách bảo mật, cần trả lời các câu hỏi:

1. What resources are you trying to protect? (chúng ta đang cố gắng bảo vệ tài nguyên nào): Câu trả lời không phải lúc nào cũng rõ ràng. Máy tính, cpu hay máy chủ lưu trữ…. Nếu tài nguyên là các tệp quan trọng, chũng ta cần các xác thực nhiều lớp, mật khẩu, hay mã hóa chúng….
2. Who is interested in attacking you ? (ai quan tâm tới việc tấn công bạn?):
3. How much security can you afford? (khả năng của bạn cho bảo mật là bao nhiêu?): chi phí về phần cứng, nhân sự, sự bất tiện khi gia tăng an ninh…..

anything you don't understand is dangerous until you do understand it - Beowulf Schaefer in Flatlander —LARRY NIVEN

Tường lửa là công cụ hiệu quả để bảo vệ hệ thống nội bộ khỏi các nguy cơ an an toàn mạng trong khi cho phép kết nối với thế giới bên ngoài thông qua mạng diện rộng hoặc Internet

1. Sự cần thiết của tường lửa

Hệ thống thông tin của các doanh nghiệp, chính phủ hay các tổ chức đã trải qua một thời gian để phát triển và tiến hóa. Sau đây là những lưu ý khi phát triển hệ thống:

* Hệ thống xử lí dữ liệu tập trung, với một Central Mainframe hỗ trợ một số thiết bị đầu cuối kết nối trực tiếp.
* Các mạng cục bộ (LAN) kết nối các PC với nhau và kết nối vowsu mainframe.
* Mạng cơ sở, bao gồm các mạng LAN, máy tính, máy chủ và một Mainfame hoặc hai[…(Premise networks)](http://www.timbercon.com/premise-networks/)
* Mạng toàn doanh nghiệp, …

# Đặc tính của tường lửa và chính sách truy cập (Access policy).

[BELL94] Danh sách mục đich thiết kế tường lửa:

1. Tất cả mọi traffic từ trong ra ngoài hay ngược lại để phải qua tường lửa. Điều này thực hiện bằng cách chặn tất cả mọi truy cập vào mạng cục bộ, ngoài trừ thông qua tường lửa.
2. Chỉ những traffic được phép, hay được xác định bới chính sách bảo mật cục bộ mới được phép thông qua.
3. Tường lửa phải miễn dịch với mọi xâm nhập. Có nghĩa là tường lửa sử dụng một hệ thống cứng và một hệ điều hành an toàn.

Đây chỉ là design goals, tường lửa nên được thiết kế đảm bảo các tiêu chí này, nếu có tiêu chí nào không đảm bảo thì đó là tường lửa yếu.

Một thành phần quan trọng trong việc lập kế hoạch và thực hiện tường lửa là chỉ định chính sách truy cập phù hợp. Danh sách này liệt kê các loại lưu lượng truy cập được ủy quyền để vượt qua tường lửa, bao gồm dải địa chỉ, giao thức, ứng dụng và nội dung loại. Chính sách này nên được xây dựng từ chính sách và đánh giá rủi ro an ninh thông tin của tổ chức mà chúng ta thảo luận trong . Chính sách này nên được phát triển từ đặc điểm kỹ thuật rộng về loại lưu lượng truy cập mà tổ chức cần hỗ trợ. Sau đó nó được tinh chỉnh để chi tiết các phần tử lọc mà chúng ta thảo luận tiếp theo, mà sau đó có thể được triển khai trong một cấu trúc liên kết tường lửa thích hợp.

Các đặc tính mà tường lửa có thể sử dụng để lọc traffic.

IP address và giao thức: lọc các giao thức tâng ứng dụng, sử dụng một application-level gateway.

User indentity: (danh tính người dùng); thowngf dùng cho người dùng bên trọng sử dụng để tự nhận dạng mình bằng các công nghệ xác thực bảo mật ví dụ như ipsec.

Hoạt động của mạng: kiểm soát dựa trên thời gian hoặc các yêu cầu: ví dụ chỉ hoạt động trong giờ hành chính ….

Tổng kết về tường lửa:

Tường lửa định nghĩa một điểm choke (cổ chai, thắt nút, điểm nút) cố gắng ngăn người dùng không được phép ra khỏi mạng được bảo vệ, cấm các dịch vụ dễ bị tổn thương xâm nhập hoặc rời khỏi mạng và cung cấp sự bảo vệ từ các loại tấn công IP spoofing và routing attack. Việc sử dụng một điểm choke đơn giản hóa việc quản lý bảo mật vì các khả năng bảo mật được hợp nhất trên một hệ thống hoặc một tập hợp các hệ thống.

Tường lửa là một nơi để theo dõi các sự kiện liên quan đến bảo mật. kiểm tra, cảnh báo đều có thể thực hiện trên tường lửa.

Tường lửa cũng có thể là một nền tảng thuận tiện cho một số các chức năng không liên quan tới bảo mật, ví dụ như NAT..

Tường lửa có thể sử dụng làm nền tảng cho IPSEC, sử dụng khả năng tạo turnnel. (chap 22)

Hạn chế của tường lửa:

1. Tường lửa không thể bảo vệ các cuộc tấn công bypass qua tường lửa. Hệ thống mạng cục bộ có thể có các kết nối tời Isp thông qua dial-out…
2. Tương lửa không thể ngăn chặn các nguy cơ từ bên trong nội bộ (tấn công từ bên trong)
3. Một wireless Lan có thể được truy cập từ bên ngoài, tường lửa phân tách các mạng doanh nghiệp không thể bảo vệ các….( An improperly secured wireless LAN may be accessed from outside the  
   organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall)
4. Laptop, pda, các thiết bị lưu trữ di động có thể bị lây nhiễm từ bên ngoài.

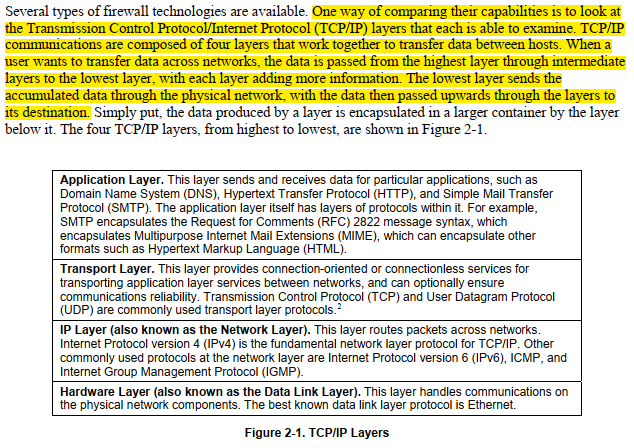
## Firewall Limitations

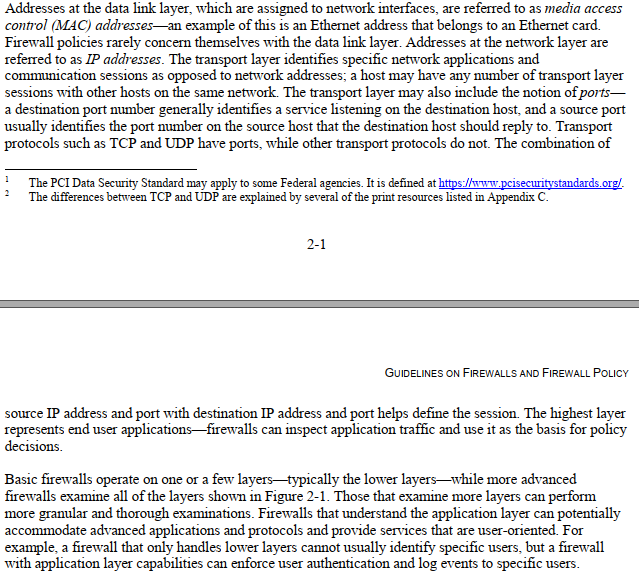
A firewall is a crucial component of securing your network and is designed to address the issues of data integrity or traffic authentication (via stateful packet inspection) and confidentiality of your internal network (via NAT). Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. The importance of including a firewall in your security strategy is apparent; however, firewalls do have the following limitations:

* A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
* Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.
* Firewalls are ineffective against nontechnical security risks such as social engineering, as discussed in Chapter 1, “There Be Hackers Here.”
* Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
* Firewalls cannot protect you from poor decisions.
* Firewalls cannot protect you when your security policy is too lax.

cisco

William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin-Firewalls and Internet Security\_ Repelling the Wily Hacker-Addison-Wesley Professional





# Phân loại tường lửa:

Tường lửa có thể giám sát lưu lượng tại một số tầng khác nhau. Có 4 loại tường lửa chính: packet filtering, circuit gateways, and application gateways.

## packet filtering firewall.

Hoạt động bằng cách xóa các gói tin dựa theo địa chỉ nguồn, đích hoặc cổng của chúng. Khi gói tin tới, nó áp dụng mộ bộ quy tắc để xác định chuyển tiếp hay loại bỏ gói và nó được thiết kế để lọc thông tin từ cả hai hướng: từ trong ra ngoài và ngược lại. Các quy tắc lọc dựa trên các thông tin:

* địa chỉ IP nguồn.
* địa chỉ ip đích.
* Giao thức truyền tải được sử dụng : TCp, udp..
* Các đặc điểm của transport-layer : source session hay destination port.
* Interface.

Pagket filtering thường được thiết lập dưới dạng một danh sách các quy tắc đặt lên các trường trong TCP/IP header. Nếu một gói tin có kết quả trùng với 1 quy tắc, quy tắc đó sẽ được gọi để xác định xem có chuyển tiếp hay hủy gói. Nếu không trùng với bất cứ quy tắc nào thì chính sách mặc định sẽ được thực hiện. Có hai chính sách mặc định:

* Default = discard: loại bỏ.
* Deafult = forward: chuyển tiếp.

Tùy theo tổ chức mà sử dụng các chính sách mặc định khác nhau. Ví dụ như các doanh nghiệp, ngân hàng,… thường ưu tiên sử dụng discard trong khi các tổ chức “mở” hơn sử dụng forward ví dụ như trường đại học..

Ưu điểm của packet filtering firewall nằm ở tính đơn giản của nó, nó cũng hoặt động rất nhanh.

Điểm yếu của nó là: [SCAR09b]

* Vì packet filtering không kiểm tra dữ liệu của các upper-data layer (5-7 trong osi) nên không thể ngăn chặn các cuộc tấn công lỗ hổng ứng dụng hay sử dụng các chức năng của ứng dụng. Nếu packet filter firewall cho phép 1 ứng dụng, mọi hàm của nó đều được cho phép.
* Log hạn chế thông tin do packet filter xử lí ít thông tin. Nó chỉ cung cấp các thông tin về nguồn, đích, loại lưu lượng.
* Đa phần các firewall loại này không hỗ trợ xác thực người dùng.
* Packet filter firewalls are generally vulnerable to attacks and exploits that take  
  advantage of problems within the TCP/IP specification and protocol stack,  
  such as network layer address spoofing. Many packet filter firewalls cannot  
  detect a network packet in which the OSI Layer 3 addressing information has  
  been altered. Spoofing attacks are generally employed by intruders to bypass  
  the security controls implemented in a firewall platform
* Vì sử dụng số lượng ít tông tin trong kiemer soát truy cập nên nó rất khó trong việc cấu hình chính xác.

Một số loại tấn công có thể thực hiện trên tường lửa lọc gói tin:

* IP address spoofing
* Source routing attacks
* Tiny flagment attacks.

## tường lửa lớp ứng dụng (application-level gateway).

Application-level gateway còn được gọi là proxy, hoạt động để chuyển tiếp lưu lượng của ứng dụng.