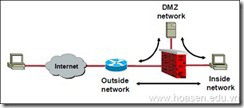
1.1 Định nghĩa firewall

Thuật ngữ firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ thông tin, firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống nhằm mục đích phá hoại, gây tổn thất cho tổ chức, doanh nghiệp. Cũng có thể hiểu firewall là một cơ chế để bảo vệ mạng tin tưởng (trusted network) khỏi các mạng không tin tưởng (untrusted network).

[](http://nguyentanvy.files.wordpress.com/2011/11/clip_image0021.jpg)

Mô hình firewall cơ bản

1.2 Những chức năng chính của firewall

Về cơ bản firewall có khả năng thực hiện các nhiệm vụ sau đây:

* Quản lý và điều khiển luồng dữ liệu trên mạng.
* Xác thực quyền truy cập
* Hoạt động như một thiết bị trung gian
* Bảo vệ tài nguyên
* Ghi nhận và báo cáo các sự kiện

1.2.1 Quản lý và kiểm soát luồng dữ liệu trên mạng

Việc đầu tiên và cơ bản nhất mà tất cả các firewall đều có là quản lý và kiểm soát luồn dữ liệu trên mạng, firewall kiểm tra các gói tin và giám sát các kết nối đang thực hiện và sau đó lọc các kết nối dựa trên kết quả kiểm tra gói tin và các kết nối được giám sát.

- Packet inspection (kiểm tra gói tin) là quá trình chặn và xử lý dữ liệu trong một gói tin để xác định xem nó được phép hay không được phép đi qua firewall. Kiểm tra gói tin có thể dựa vào các thông tin sau:

* Địa chỉ IP nguồn
* Port nguồn.
* Địa chỉ IP đích
* Port đích
* Giao thức IP
* Thông tin trong header (sequence numbers, checksums, data flags, payload information…)

- Connections và state: Khi hai TCP/IP host muốn giao tiếp với nhau, chúng cần thiêt lập một số kết nối với nhau. Các kết nối phục vụ hai mục đích. Thứ nhất, nó dùng để xác thực bản thân các host với nhau. Friewall dùng các thông tin kết nối này để xác định kết nối nào được phép và các kết nối nào không được phép.Thứ hai, các kết nối dùng để xác định cách thức mà hai host sẽ liên lạc với nhau (dùng TCP hay dùng UDP…).

- Stateful Packet Inspection (giám sát gói tin theo trạng thái): Statefull packet inspection không những kiểm tra gói tin bao gồm cấu trúc, dữ liệu gói tin … mà kiểm tra cả trạng thái gói tin.

1.2.2 Xác thực quyền truy cập

Firewall có thể xác thực quyền truy cập bằng nhiều cơ cấu xác thực khác nhau. Thứ nhất, firewall có thể yêu cầu username và password của người dùng khi người dùng truy cập (thường được biết đến như là extended authentication hoặc xauth). Sau khi firewall xác thực xong người dùng, firewall cho phép người dùng thiết lập kết nối và sau đó không hỏi username và password lại cho các lần truy cập sau (thời gian firewall hỏi lại username và password phụ thuộc vào cách cấu hình của người quản trị). Thứ hai, firewall có thể xác thực người dùng bằng certificates và public key. Thứ ba, firewall có thể dùng pre-shared keys (PSKs) để xác thực người dùng.

1.2.3 Hoạt động như một thiết bị trung gian

Khi user thực hiện kết nối trực tiếp ra bên ngoài sẽ đối mặt với vô số nguy cơ về bảo mật như bị virus tấn công, nhiễm mã độc hại… do đó việc có một thiết bị trung gian đứng ra thay mặt user bên trong để thực hiện kết nối ra bên ngoài là cần thiết để đảm bảo an toàn. Firewall được cấu hình để thực hiện chức năng này và firewall được ví như một proxy trung gian.

1.2.4 Bảo vệ tài nguyên

Nhiệm vụ quan trọng nhất của một firewall là bảo vệ tài nguyên khỏi các mối đe dọa bảo mật. Việc bảo vệ này được thực hiện bằng cách sử dụng các quy tắc kiểm soát truy cập, kiểm tra trạng thái gói tin, dùng application proxies hoặc kết hợp tất cả để bảo vệ tài nguyên khỏi bị truy cập bất hợp pháp hay bị lạm dụng. Tuy nhiên, firewall không phải là một giải pháp toàn diện để bảo vệ tài nguyên của chúng ta.

1.2.5 Ghi nhận và báo cáo các sự kiện

Ta có thể ghi nhận các sự kiện của firewall bằng nhiều cách nhưng hầu hết các firewall sử dụng hai phương pháp chính là syslog và proprietaty logging format. Bằng cách sử dụng một trong hai phương pháp này, chúng ta có thể dễ dàng báo cáo các sự kiện xẩy ra trong hệ thống mạng.

### **3. Các thành phần cơ bản của firewall và cơ chế hoạt động**

Một firewall bao gồm một hoặc nhiều thành phần sau đây:

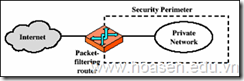
* Packet Filtering – Bộ lọc gói tin
* Application Gateway – Cổng ứng dụng
* Circuit Level Gate – Cổng mạch

#### 3.1 Packet Filtering

##### 3.1.1 Nguyên lý hoạt động

Bộ lọc gói tin cho phép hay từ chối packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong các số các rules hay không. Các rules này dựa trên các thông tin ở packet header bao gồm các thông tin sau:

* Địa chỉ IP nguồn (IP Source Address).
* Địa chỉ IP đích (IP Destination Address).
* Protocol (TCP, UDP, ICMP, IP tunnel)
* TCP/UDP source port
* TCP/UDP destination port
* Dạng thông báo ICMP (ICMP message type)
* Cổng gói tin đến (Incomming interface of packet)
* Cổng gói tin đi (Outcomming interface of packet)

[](http://nguyentanvy.files.wordpress.com/2011/11/clip_image012.png)

Packet filtering router

Nếu rules lọc gói được thỏa mãn thì packet được chuyển qua firewall, nếu không packet sẽ bị bỏ đi. Nhờ vậy mà firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó hoặc những dịch vụ nào đó (SSH, SMTP, FTP…) được phép mới chạy được trên hệ thống mạng cục bộ.

#### 3.2 Application Gateway

##### 3.2.1 Nguyên lý hoạt động

Đây là một loại firewall được thiết kế dể tăng cường chức năng kiểm soát các loại dịch vụ, giao thức truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là proxy service. Proxy service là các bộ code đặc biệt cài đặt trên cổng ra (gateway) cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy service cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị cho là chấp nhận được trong khi từ chối những đặc điểm khác.

[](http://nguyentanvy.files.wordpress.com/2011/11/clip_image014.jpg)

Application gateway

Một cổng ứng dụng thường được coi như là một Bastion host bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một Bastion host là:

- Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ điều hành (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào hệ điều hành (Operating system) cũng như là đảm bảo sự tích hợp firewall.

- Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên Bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên Bastion host.

- Bastion host có thể yêu cầu nhiều mức độ khác nhau ví dụ như username và password hay smart card.

Mỗi proxy được cài đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

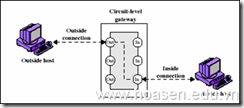
Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của dữ liệu mạng đi qua nó. Điều này có nghĩ là bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy đều độc lập với các proxy khác trên Bastion host. Điều này cho phép dễ dàng cài đặt một proxy mới hay tháo gỡ một proxy.

#### 3.3 Circuit Level Gateway

Circuit Level Gateway – cổng vòng – là một chức năng đặc biệt có thể thực hiện bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ là chuyển tiếp các kết nối TCP mà không thực hiện bất kì một hành động xử lý hay lọc gói nào.

Hình sau minh họa một hành động sử dụng kết nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên vì sự kết nối này xuất hiện từ hệ thống firewall nên nó che dấu thông tin về mạng nội bộ.

[](http://nguyentanvy.files.wordpress.com/2011/11/clip_image015.png)

Circuit Level Gateway

Cổng vòng thường được sử dụng cho những kết nối ra ngoài. Ưu điểm lớn nhất là một Bastion host có thể được cấu hình như là một hỗn hợp cung cấp cổng ứng dụng cho những kết nối đến và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống firewall dễ dàng sử dụng cho người dùng trong mạng nội bộ muốn trực tiếp truy câp tới các dịch vụ internet, trong khi vẫn cung cấp chức năng bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

**Firewall là gì ?**  
  
Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật đ­ợc tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Cũng có thể hiểu Firewall là một cơ chế (mechanism) để bảo vệ mạng tin t­ởng (Trusted network) khỏi các mạng không tin t­ởng (Untrusted network).  
  
Thông th­ờng Firewall đ­ợc đặt giữa mạng bên trong (Intranet) của một công ty, tổ chức, ngành hay một quốc gia, và Internet. Vai trò chính là bảo mật thông tin, ngăn chặn sự truy nhập không mong muốn từ bên ngoài (Internet) và cấm truy nhập từ bên trong (Intranet) tới một số địa chỉ nhất định trên Internet.  
  
**Chức năng chính**  
  
Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:  
  
Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).   
Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).   
Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.   
Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.   
Kiểm soát ng­ời sử dụng và việc truy nhập của ng­ời sử dụng.   
Kiểm soát nội dung thông tin thông tin l­u chuyển trên mạng.   
Các thành phần  
  
Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:  
  
Bộ lọc packet (packet-filtering router)   
Cổng ứng dụng (application-level gateway hay proxy server)   
Cổng mạch (circuite level gateway)   
Bộ lọc paket (Paket filtering router)  
  
**Nguyên lý**  
  
Khi nói đến việc l­u thông dữ liệu giữa các mạng với nhau thông qua Firewall thì điều đó có nghĩa rằng Firewall hoạt động chặt chẽ với giao thức TCI/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận đ­ợc từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data pakets) rồi gán cho các paket này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các packet và những con số địa chỉ của chúng.  
  
Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận đ­ợc. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:  
  
Địa chỉ IP nơi xuất phát ( IP Source address)   
Địa chỉ IP nơi nhận (IP Destination address)   
Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)   
Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)   
Cổng TCP/UDP nơi nhận (TCP/UDP destination port)   
Dạng thông báo ICMP ( ICMP message type)   
Giao diện packet đến ( incomming interface of packet)   
Giao diện packet đi ( outcomming interface of packet)   
Nếu luật lệ lọc packet đ­ợc thoả mãn thì packet đ­ợc chuyển qua firewall. Nếu không packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản đ­ợc các kết nối vào các máy chủ hoặc mạng nào đó đ­ợc xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) đ­ợc phép mới chạy đ­ợc trên hệ thống mạng cục bộ.  
  
  
  
**Những hạn chế của firewall**  
  
Firewall không đủ thông minh nh­ con ng­ời để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nh­ng phải xác định rõ các thông số địa chỉ.   
Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đ­ờng dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.   
Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack). Khi có một số ch­ơng trình đ­ợc chuyển theo th­ điện tử, v­ợt qua firewall vào trong mạng đ­ợc bảo vệ và bắt đầu hoạt động ở đây.   
Một ví dụ là các virus máy tính. Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu đ­ợc chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của firewall.   
Tuy nhiên, Firewall vẫn là giải pháp hữu hiệu đ­ợc áp dụng rộng rãi.