**ĐẠI HỌC HUẾ**



**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**KHOA CÔNG NGHỆ THÔNG TIN**

**MÔN AN NINH MẠNG**

**- - - 🙞 🕮** **🙜 - - -**

**ĐỀ TÀI**

**TÌM HIỂU VỀ HỆ THỐNG TƯỜNG LỬA**

**(FIREWALL)**



**Giáo viên hướng dẫn: Võ Việt Dũng**

**Sinh viên thực hiện :**

**Trần Khánh (Nhóm trưởng)**

**Lê Ngọc Minh**

**Nguyễn Tiến Dũng**

**Nguyễn Bá Quý Đạt**

**Võ Hữu Lộc**

**MỤC LỤC**

**LỜI NÓI ĐẦU**

**CHƯƠNG I: TỔNG QUAN VỀ FIREWALL**

1. Khái niệm
2. Chức năng
3. Phân loại

3.1 Firewall cứng

3.2 Firewall mềm

1. Nguyên lý hoạt động của Firewall
2. Ứng dụng của Firewall

5.1 Firewall bảo vệ cái gì?

5.2 Firewall chống lại cái gì?

**CHƯƠNG II: NHỮNG THIẾT KẾ CƠ BẢN CỦA FIREWALL**

1. Dual-homed Host
2. Kiến trúc screened Host
3. Kiến trúc Screened Subnet Host
4. Sử dụng nhiều Bastion Host
5. Kiến trúc ghép chung Router trong và Router ngoài
6. Kiến trúc ghép chung Bastion Host và Router ngoài

**CHƯƠNG III: CÁC THÀNH PHẦN VÀ CƠ CHẾ HOẠT ĐỘNG**

**CỦA FIREWALL**

1. Bộ lọc gói (Packet Filtering)

1.1 Nguyên lý hoạt động

1.2 Ưu điểm và hạn chế của hệ thống Firewall sử dụng bộ lọc Packet

1. Cổng ứng dụng (Application-Level Gateway)

2.1 Nguyên lý hoạt động

2.2 Ưu điểm và hạn chế

1. Cổng vòng (Circuit-Level Gateway)

**CHƯƠNG IV: CÁC CÔNG NGHỆ TƯỜNG LỬA HIỆN NAY**

1. Một số công nghệ tường lửa hiện nay
2. Tổng kết

**CHƯƠNG V: KẾT LUẬN**

**LỜI NÓI ĐẦU**

An toàn thông tin là nhu cầu rất quan trọng đối với cá nhân cũng như đối với xã hội và các quốc gia trên thế giới. Mạng máy tính an toàn thông tin được tiến hành thông qua các phương pháp vật lý và hành chính. Từ khi ra đời cho đến nay mạng máy tính đã đem lại hiệu quả vô cùng to lớn trong tất cả các lĩnh vực của đời sống. Bên cạnh đó người sử dụng phải đối mặt với các hiểm họa do thông tin trên mạng của họ bị tấn công. An toàn thông tin trên mạng máy tính bao gồm các phương pháp nhằm bảo vệ thông tin được lưu giữ và truyền trên mạng. An toàn thông tin trên mạng máy tính là một lĩnh vực đang được quan tâm đặc biệt đồng thời cũng là một công việc hết sức khó khăn và phức tạp. Thực tế đã chứng tỏ rằng có một tình trạng rất đáng lo ngại khi bị tấn công thông tin trong quá trình xử lý, truyền và lưu giữ thông tin. Những tác động bất hợp pháp lên thông tin với mục đích làm tổn thất, sai lạc, lấy cắp các tệp lưu giữ tin, sao chép các thông tin mật, giả mạo người được phép sử dụng thông tin trong các mạng máy tính.

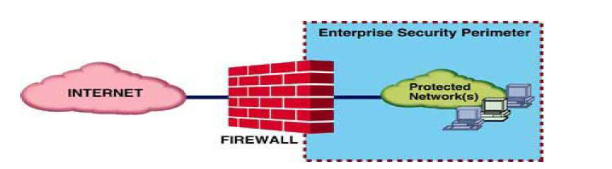
Tường lửa không chỉ là một dạng phần mềm (như tường lửa trên Windows), mà nó còn có thể là phần cứng chuyên dụng trong các mạng doanh nghiệp. Các tường lửa là phần cứng này giúp máy tính của các công ty có thể phân tích dữ liệu ra để đảm bảo rằng malware không thể thâm nhập vào mạng, kiểm soát hoạt động trên máy tính mà nhân viên của họ đang sử dụng. Nó cũng có thể lọc dữ liệu để chỉ cho phép một máy tính chỉ có thể lướt web, vô hiệu hóa việc truy cập vào các loại dữ liệu khác.

Với sự hướng dẫn giảng viên Võ Việt Dũng, nhóm em đã hoàn thành bài báo cáo này. Tuy đã cố gắng hết sức tìm hiểu, phân tích nhưng chắc rằng không tránh khỏi những thiếu sót. Nhóm em rất mong nhận được sự thông cảm và góp ý của quý thầy cô và các bạn.

**CHƯƠNG I: TỔNG QUAN VỀ FIREWALL**

**1. Khái niệm**

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 đề chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhâp không mong muốn vào hệ thống. Firewall được miêu tả như là hệ phòng thủ bao quanh với các “chốt” để kiểm soát tất cả các luồng lưu thông nhập xuất. Có thể theo dõi và khóa truy cập tại các chốt này.



Các mạng riêng nối với Internet thường bị đe dọa bởi những kẻ tấn công. Để bảo vệ dữ liệu bên trong người ta thường dùng Firewall. Firewall có cách nào đó để cho phép người dùng hợp lệ đi qua và chặn lại những người dùng không hợp lệ. Firewall có thể là thiết bị phần cứng hoặc chương trình phần mềm chạy trên host bảo đảm hoặc kết hợp cả hai. Trong mọi trường hợp, nó phải có ít nhất hai giao tiếp mạng, một cho mạng mà nó bảo vệ, một cho mạng bên ngoài. Firewall có thể là gateway hoặc điểm nối liền giữa hai mạng, thường là một mạng riêng và một mạng công cộng như là Internet. Các firewall đầu tiên là các router đơn giản.

**2. Chức năng**

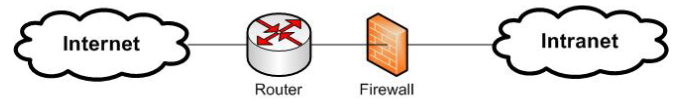
Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:

* 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 người sử dụng và việc truy nhập của người sử dụng.
* Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.

**3. Phân loại**

**3.1 Firewall cứng**

Tường lửa phần cứng là một lựa chọn hợp lý nếu bạn đang dùng các phiên bản Windows trước đây. Nhiều điểm truy cập (access point) không dây sử dụng cho các mạng gia đình đều được đóng gói dưới dạng tổng hợp tất cả-trong-một, tích hợp các tường lửa phần cứng với các broadband router. Việc dùng một tường lửa cho hệ thống mạng của bạn có thể đơn giản như việc thêm một máy trả lời điện thoại vào đường dây điện thoại của bạn. Bạn chỉ cần đặt tường lửa vào kết nối Ethernet giữa modem cáp/DSL và máy tính của bạn. (Đúng với hầu hết các loại tường lửa).



Đặc điểm của Firewall cứng:

* Không được linh hoạt như Firewall mềm: (Không thể thêm chức năng, thêm quy tắc như firewall mềm).
* Có thể quản lý tập trung.
* Đơn giản, dễ lắp đặt, cấu hình, quản lý.
* Firewall cứng hoạt động ở tầng thấp hơn Firewall mềm (Tầng Network và tầng Transport).
* Firewall cứng không thể kiểm tra được nội dung của gói tin.

Ví dụ Firewall cứng: NAT (Network Address Translate).

**3.2 Firewall mềm**

Có rất nhiều nhà cung cấp Tường lửa phần mềm mà bạn có thể sử dụng nếu bạn dùng các phiên bản Windows trước đây. Các nhà cung cấp cũng có các loại tường lửa khác có thể sử dụng trên Windows XP. Dưới đây là danh sách một số nhà cung cấp:

* Internet Security Systems (ISS): BlackICE PC Protection.
* Network Associates: McAfee Personal Firewall.
* Symantec: Norton Personal Firewall.
* Tiny Software: Tiny Personal Firewall.
* Zone Labs: ZoneAlarm.

Đặc điểm của Firewall mềm: Tính linh hoạt cao như là có thể thêm, bớt các quy tắc, các chức năng. Firewall mềm hoạt động ở tầng cao hơn Firewall cứng (tầng ứng dụng) Firewall mềm có thể kiểm tra được nội dung của gói tin (thông qua các từ khóa).

Ví dụ về Firewall mềm: ZoneAlarm, Norton Firewall ...

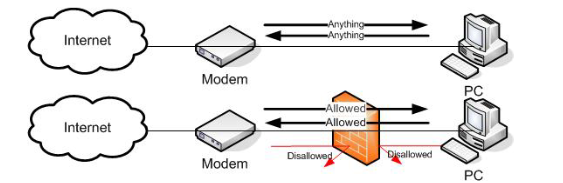
**4. Nguyên lý hoạt động của Firewall**

Firewall hoạt động chặt chẽ với giao thức TCP/IP, vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMTP, NFS ... ) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ 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 được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa 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 (header), dùng để cho phép truyền các packet đó ở trên mạng. Bao gồm:

* Địa chỉ IP nơi xuất phát (Source)
* Địa chỉ IP nơi nhận ( Destination)
* Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel ... )
* Cổng TCP/UDP nơi xuất phát
* Cổng TCP/UDP nơi nhận
* Dạng thông báo ICMP
* Giao diện packet đến
* Giao diện packet đi

Nếu packet thỏa các luật lệ đã được thiết lập trước của Firewall thì packet đó được chuyển qua, nếu không thỏa thì sẽ bị loại bỏ. Việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định được phép mới vào được hệ thống mạng cục bộ. Cũng nên lưu ý là do việc kiểm tra dựa trên header của các packet nên bộ lọc không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu. Trong các phần sau chúng ta sẽ cùng tìm hiểu các kỹ thuật để vượt tường lửa.

**5. Ứng dụng của Firewall**



Nếu máy tính của bạn không được bảo vệ, khi bạn kết nối Internet, tất cả các giao thông ra vào mạng đều được cho phép, vì thế hacker, trojan, virus có thể truy cập và lấy cắp thông tin cá nhân của bạn trên máy tính. Chúng có thể cài đặt các đoạn mã để tấn công file dữ liệu trên máy tính. Chúng có thể sử dụng máy tính của bạn để tấn công một máy tính của gia đình hoặc doanh nghiệp khác kết nối Internet. Một firewall có thể giúp bạn thoát khỏi gói tin hiểm độc trước khi nó đến hệ thống của bạn.

**5.1 FireWall bảo vệ cái gì ?**

Nhiệm vụ cơ bản của FireWall là bảo vệ những vấn đề sau :

* Dữ liệu: Những thông tin cần được bảo vệ do những yêu cầu về tính bảo mật, tính toàn vẹn và tính kịp thời.
* Tài nguyên hệ thống.
* Danh tiếng của công ty sở hữu các thông tin cần bảo vệ.

**5.2 FireWall bảo vệ chống lại cái gì ?**

Firewall là hệ thống bảo vệ chống lại những sự tấn công từ bên ngoài.

Tấn công trực tiếp:

* Cách thứ nhất là dùng phương pháp dò mật khẩu trực tiếp. Thông qua các chương trình dò tìm mật khẩu với một số thông tin về người sử dụng như ngày sinh, tuổi, địa chỉ v.v ... và kết hợp với thư viện do người dùng tạo ra, kẻ tấn công có thể dò được mật khẩu của bạn. Trong một số trường hợp khả năng thành công có thể lên tới 30%. Ví dụ nhu chương trình do tìm mật khẩu chạy trên hệ điều hành Unix có tên là \*\*\*\*\*
* Cách thứ hai là sử dụng lỗi của các chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được để chiếm quyền truy cập (có được quyền của người quản trị hệ thống).

Nghe trộm: Có thể biết được tên, mật khẩu, các thông tin chuyền qua mạng thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền qua mạng.

Giả mạo địa chỉ IP: Là Hacker thường dùng cách này để mạo danh là máy tính hợp pháp nhằm chiếm quyền điều khiển trình duyệt web trên máy tính bị tấn công.

Vô hiệu hóa các chức năng của hệ thống (deny service): Đây là kiểu tấn công nhằm làm tê liệt toàn bộ hệ thống không cho nó thực hiện các chức năng mà nó được thiết kế. Kiểu tấn công này không thể ngăn chặn được do những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

Lỗi người quản trị hệ thống: Yếu tố con người với những tính cách chủ quan và không hiểu rõ tầm quan trọng của việc bảo mật hệ thống nên dễ dàng để lộ các thông tin quan trọng cho hacker. Ngày nay, trình độ của các hacker ngày càng giỏi hơn, trong khi đó các hệ thống mạng vẫn còn chậm chạp trong việc xử lý các lỗ hổng của mình. Điều này đòi hỏi người quản trị mạng phải có kiến thức tốt về bảo mật mạng để có thể giữ vững an toàn cho thông tin của hệ thống. Đối với người dùng cá nhân, họ không thể biết hết các thủ thuật để tự xây dựng cho mình một Firewall, nhưng cũng nên hiểu rõ tầm quan trọng của bảo mật thông tin cho mỗi cá nhân, qua đó tự tìm hiểu để biết một số cách phòng tránh những sự tấn công đơn giản của các hacker. Vấn đề là ý thức, khi đã có ý thức để phòng tránh thì khả năng an toàn sẽ cao hơn.

**CHƯƠNG II: NHỮNG THIẾT KẾ CƠ BẢN CỦA FIREWALL**

**1. Dual-homed Host**

Firewall kiến trúc kiểu Dual-homed host được xây dựng dựa trên máy tính dual-homed host. Một máy tính được gọi là dual-homed host nếu nó có ít nhất hai network interface, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau, do đó máy tính này đóng vai trò là router mềm. Kiến trúc dua1 - homed host rất đơn giản, máy dual - homed host ở giữa, một bên được nối với internet và bên còn lại nối với mạng nội bộ (mạng cần được bảo vệ).

Gồm có các đặc điểm sau:

* Phải disable chức năng routing của dual-homed host để cấm hòan toàn lưu thông IP từ ngoài vào.
* Các hệ thống bên trong và bên ngoài dual-homed host chỉ có thể liên lạc với dua1-homed host mà chúng không liên lạc trực tiếp được với nhau.
* Dual-homed host cung cấp dịch vụ thông qua proxy server hoặc login trực tiếp vao dual-homed host.

**2. Kiến trúc Screened Host**

Trong kiến trúc này chức năng bảo mật chính được cung cấp bởi chức năng packet filtering tại screening router.

Packet filtering trên screening router được setup sao cho bastion host là máy duy nhất trong internal network mà các host trên internet có thể mở kết nối đến.Packet filtering cũng cho phép bastion host mở các kết nối(hợp pháp) ra bên ngoài(external network).

Thường Packet filtering thực hiện các công việc như sau :

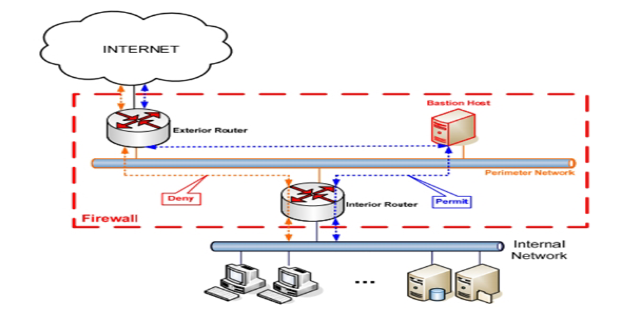
* Cho phép các internal hosts mở kết nối đến các host trên internet đối với một số dịch vụ được phép.
* Cấm tất cả kết nối từ các internal hosts .

Khi hacker đã tấn công được vào bastion host thì không còn một rào chắn nào cho các internal hosts.

**3. Kiến trúc Screened Subnet Host**

Thêm môt perimeter network để cô lập internal network với internet. Như vậy dù hacker đã tấn công được vào bastion host vẫn còn một rào chắn nữa phải vượt qua là interior router. Các lưu thông trong internal network được bảo vệ an toàn cho dù bastion đã bị"chiếm”. Các dịch vụ nào ít tin cậy và có khả năng dễ bị tấn công thì nên để ở perimeter network. Bastion host là điểm liên lạc cho các kết nối từ ngoài vào như: SMTP; FTP, DNS. Còn đối với việc truy cập các dịch vụ từ internal clients đến các server trên internet thì được điều khiển như sau :

* Set up packet filtering trên cả hai exterior và interior router để cho phép internal clients truy cập các servers bên ngoài một cách trực tiếp.
* Set up proxy server trên bastion host để cho phép internal clients truy cập các servers bên ngoài một cách gián tiếp.



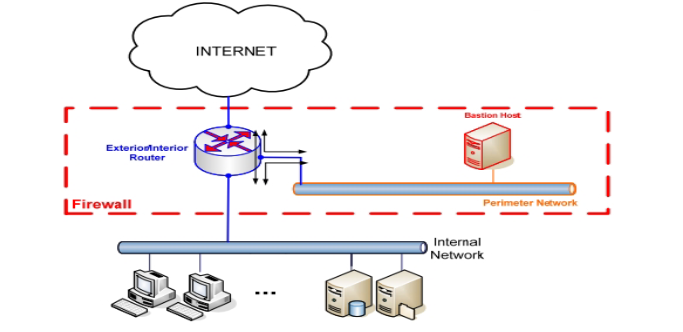
**4. Sử dụng nhiều Bastion Host**

Với mô hình này thì tốc độ đáp ứng cho những người sử dụng bên trong (local user) một phần nào đó không bị ảnh hưởng bởi những hoạt động của người sử dụng bên ngoài mạng (external user).

**5. Kiến trúc ghép chung Router trong và Router ngoài**

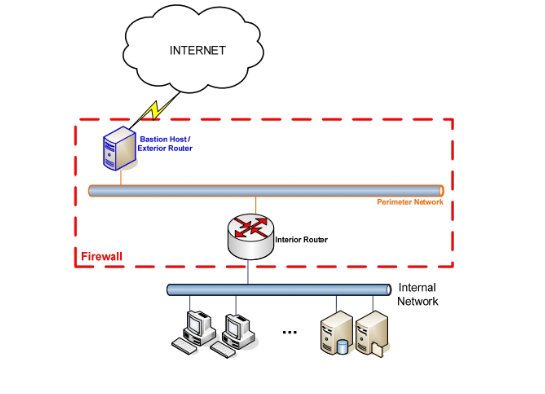
Router phải cho phép áp dụng các luật cho dòng packet đi vô và đi ra trên mỗi interface.

Do ghép chung router trong và router ngoài nên kiến trúc này làm giảm đi lớp bảo vệ mạng bên trong, có thể nói kiến trúc ghép chung router trong và router ngoài nằm ở giữa kiến trúc Screened host và Screened Subnet host.



**6. Kiến trúc ghép chung Bastion Host và Router ngoài**

Kiến trúc này chỉ sử dụng cho mạng chỉ có một đường nối dùng giao thức SLIP hoặc PPP ra internet.

Kiểu ghép chung Bastion host và router ngoài (Exterior router) này gần giống với Screened Subnet Host. Nó cho tốc độ đáp ứng thường thấp nhưng mà vẫn có thể chấp nhận được đo tốc độ đường truyền thấp, chức năng lọc của router ngoài ít, chức năng lọc gói chủ yếu là router trong.

**CHƯƠNG III: CÁC THÀNH PHẦN VÀ CƠ CHẾ HOẠT ĐỘNG CỦA FIREWALL**

**1. Bộ lọc gói (Packet Filtering)**

**1.1 Nguyên lý hoạt động**

Khi nói đến việc lưu 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 TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMTP, NFS ... ) thành các gói dữ liệu (data packet) 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 được. Nó kiểm tra toàn bộ đoạn dữ liệu đề 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 (Source)
* Địa chỉ IP nơi nhận ( Destination)
* Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel ... )
* Công TCP/UDP nơi xuất phát Công TCP/UDP nơi nhận
* Dạng thông báo ICMP
* Giao diện packet đến
* Giao diện packet đi

Nếu luật lệ lọc packet được thoả 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 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 ... ) được phép mới chạy được trên hệ thống mạng cục bộ.

1.2 Ưu điểm và hạn chế của hệ thống Firewall sử dụng bộ lọc Packet

Ưu điểm:

* Chi phí thấp vì cơ chế lọc packet đã được bao gồm trong mỗi phần mềm router.
* Ngoài ra, bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng, vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

Hạn chế:

* Việc định nghĩa các chế độ lọc package là một việc khá phức tạp, đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể có thể nhận trên mỗi trường. Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.
* Do làm việc dựa trên header của các packet, rõ ràng là bộ lọc packet không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

**2. Công ứng dụng (Application-Level Gateway)**

**2.1 Nguyên lý hoạt động**

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép 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 gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code 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 mạng cho là chấp nhận được trong khi từ chối.

Một cổng ứng dụng thường được coi như là một pháo đài (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 thống (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào 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 xác thực khác nhau, ví dụ như user password hay smart card.
* Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một sồ 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 giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.
* Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ một proxy đang có vấn đề.

**2.2 Ưu điểm và hạn chế**

Ưu điểm:

* Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.
* Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.
* Công ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.
* Luật lệ lọc filtering cho cồng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

Hạn chế: Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên công ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải công ứng dụng trên lệnh Telnet.

**3. Cổng vòng (Circuit-level gateway)**

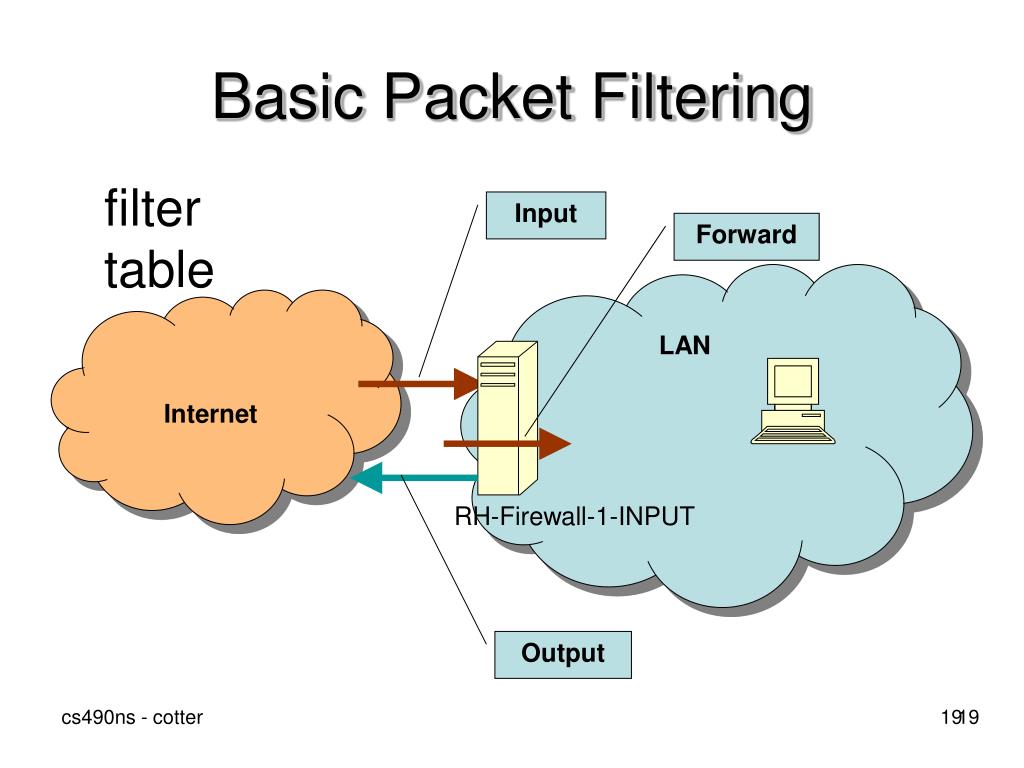
Cổng vòng là một chức năng đặc biệt có thể thực hiện được bởi một cồng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

**CHƯƠNG IV: CÁC CÔNG NGHỆ TƯỜNG LỬA HIỆN NAY**

**1. Một số công nghệ tường lửa hiện nay**

Hiện nay tường lửa đã phát triển qua nhiều thế hệ với các công nghệ khác nhau, từ cơ bản đến nâng cao, nhằm đáp ứng nhu cầu bảo mật ngày càng phức tạp. Dưới đây là các công nghệ tường lửa phổ biến:

* 1. **Packet Filtering Firewall**

****

Lọc gói tin (packet filtering) là một công nghệ bảo mật mạng. Nó liên quan đến việc kiểm tra các gói dữ liệu khi chúng di chuyển qua một thiết bị bảo mật, chẳng hạn như router hoặc tường lửa. Lợi ích của việc lọc gói tin nằm ở khả năng xác định liệu các gói tin này nên bị chặn hay được phép đi qua, dựa trên một tập hợp các quy tắc được xác định trước. Quá trình này rất quan trọng trong việc duy trì bảo mật mạng, đảm bảo rằng chỉ có dữ liệu hợp lệ mới được phép truyền qua trong khi dữ liệu có thể gây hại bị ngăn chặn.

\***Nguyên lý hoạt động:**

* + Lọc các gói dữ liệu (packets) dựa trên các thông tin cơ bản như địa chỉ IP nguồn, IP đích, cổng nguồn, cổng đích, và giao thức (TCP, UDP).
  + Dựa trên các quy tắc (rules) được cấu hình trước, tường lửa sẽ cho phép hoặc từ chối các gói tin.

\***Các kiểu lọc gói tin:**

### **1. Lọc gói tin động (Dynamic Packet Filtering)**

Lọc gói tin động, như tên gọi của nó, là một phương pháp linh hoạt trong việc lọc gói tin. Nó thích ứng với các điều kiện thay đổi của lưu lượng mạng. Loại lọc này cho phép cơ chế bảo mật phản ứng nhanh hơn, vì nó có thể điều chỉnh các tiêu chí lọc dựa trên lưu lượng mạng hiện tại và các mối đe dọa. Lọc gói tin động đặc biệt hữu ích trong các môi trường mà mô hình lưu lượng mạng liên tục thay đổi.

### **2. Lọc gói tin tĩnh (Static Packet Filtering)**

Ngược lại, lọc gói tin tĩnh đại diện cho một phương pháp cứng nhắc hơn. Nó dựa vào các quy tắc cố định, được xác định trước để lọc các gói tin. Những quy tắc này không thay đổi trừ khi được các quản trị viên mạng cập nhật thủ công. Mặc dù lọc gói tin tĩnh đơn giản và dễ quản lý hơn, nhưng nó có thể không hiệu quả bằng lọc gói tin động trong việc thích ứng với các mối đe dọa mạng mới hoặc đang phát triển.

### **3. Lọc gói tin theo trạng thái (Stateful Packet Filtering)**

Lọc gói tin theo trạng thái xem xét trạng thái của một kết nối hoặc phiên làm việc khi đưa ra các quyết định lọc. Nó theo dõi trạng thái và ngữ cảnh của các kết nối mạng, chẳng hạn như luồng TCP hoặc giao tiếp UDP, và sử dụng thông tin này để ảnh hưởng đến các quyết định lọc. Phương pháp này tinh vi hơn vì nó cho phép bộ lọc hiểu được ngữ cảnh của các gói tin, làm cho nó hiệu quả hơn trong việc nhận diện và chặn các mối đe dọa phức tạp.

### **4. Lọc gói không trạng thái (Stateless Packet Filtering)**

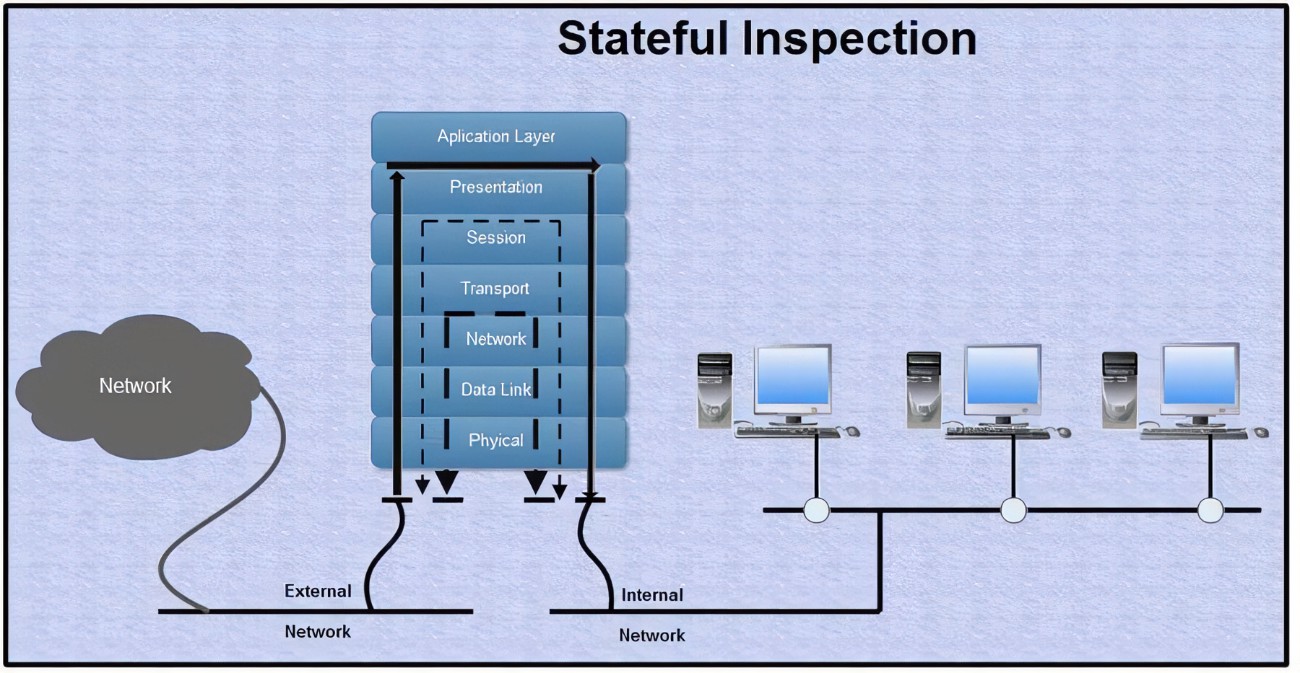
Cuối cùng, lọc gói tin không có trạng thái (stateless packet filtering) hoạt động mà không xem xét trạng thái của các kết nối mạng. Nó lọc gói tin dựa chỉ vào các quy tắc đã được xác định trước bởi các quản trị mạng, kiểm tra từng gói tin đơn lẻ. Phương pháp này ít tốn tài nguyên hơn so với lọc gói tin có trạng thái nhưng có thể không hiệu quả bằng cách xử lý các mối đe dọa tiên tiến sử dụng trạng thái hoặc ngữ cảnh của kết nối.

**\*Ưu Điểm:**

* Đơn giản, dễ triển khai và nhanh chóng.
* Hiệu quả đối với lưu lượng cơ bản.

**\*Nhược Điểm:**

* Không thể kiểm tra nội dung gói dữ liệu.
* Không bảo vệ chống lại các cuộc tấn công nâng cao như mã độc nhúng trong lưu lượng hợp lệ.
  1. **Stateful Inspection Firewall**

****

Tường lửa Stateful được xem như một loại tường lửa mạng, cũng có thể hiểu một cách đơn giản hơn nó tương tự như cái cổng quét với nhiệm vụ rà soát. Như một khâu kiểm duyệt, kiểm soát các vấn đề trong mạng, mọi thứ đều phải đi qua nó. Tường lửa Stateful như một lá chắn bảo vệ kết nối mạnh tránh sự xâm nhập của các kết nối khác ngoài quyền truy cập.

Tường lửa Stateful còn được gọi là tường lửa có trạng thái. Nó sẽ theo dõi mọi hoạt động của kết nối mạng đi qua nó. Đồng thời, còn theo dõi các đặc điểm và nhận dạng xem các gói kết nối mạng có hợp pháp hay không. Chỉ có các kết nối hợp pháp, có quyền truy cập thì mới có thể đi qua được stateful.

**\*Nguyên lí hoạt động:**

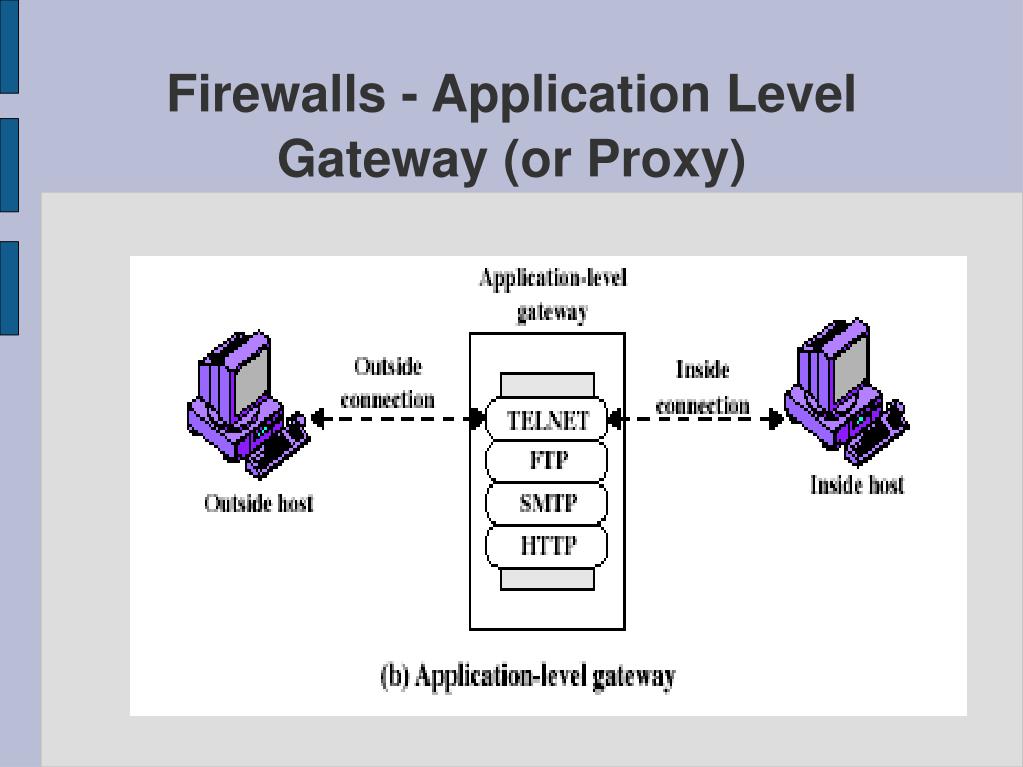
* Tường lửa sẽ lưu trữ và kiễm tra các thông tin để đánh giá quyền truy cập của kết nối. Đối với các gói tin trong quá trình giao tiếp tiếp cụ thể mà khớp với gói tin đã được thêm mục vào trong bảng trạng thái thì sẽ được thông qua và được cấp quyền truy cập mà không cần xác nhận lớp ứng dụng.
* Thông thường, các gói tin thế này chỉ cần có thông tin của lớp 3 và lớp 4 trpng việc các nhận. Những thông tin này sẽ được đối chiếu với thông tin đã lưu trong bảng trạng thái. Khi xác nhận được nó là một phần của thông tin trao đổi hiện tại thì kết nối này sẽ được cấp phép tiếp tục truy cập qua tường lửa.
* Với việc áp dụng kỹ thuật lọc như vậy, chúng không thể xem xét các lệnh lớp ứng dụng cho toàn bộ phiên truyền thông giống như một tường lửa proxy. Điều này cũng có nghĩa nó không có khả năng thực sự kiểm soát các phiên dựa trên lưu lượng truy cập cấp ứng dụng, làm nó kém an toàn hơn so với proxy. Nhưng bù lại, nó có tốc độ nhanh hơn và hoạt động tốt với khả năng xử lý bất cứ lưu lượng giao thông  nào.

**\*Ưu Điểm:**

* Hiệu quả hơn Packet Filtering vì hiểu rõ ngữ cảnh của kết nối.
* Bảo vệ tốt hơn trước các cuộc tấn công như giả mạo gói tin.

**Nhược Điểm:**

* Đòi hỏi tài nguyên xử lý nhiều hơn.
* Phức tạp hơn trong việc cấu hình và quản lý.
  1. **Proxy Firewall (Application Firewall)**

****

Tường lửa proxy cũng là máy chủ proxy. Nhưng không phải tất cả máy chủ proxy đều là tường lửa proxy. Máy chủ proxy hoạt động như một bộ máy trung gian giữa máy khách và máy chủ. Nó có thể lưu vào bộ đệm các trang web. Nhằm giảm nhu cầu băng thông, nén dữ liệu, lọc lưu lượng truy cập và phát hiện virus.

\***Nguyên lý hoạt động:**

* Hoạt động như một trung gian (proxy) giữa người dùng và tài nguyên mạng.
* Kiểm tra dữ liệu ở cấp ứng dụng, nghĩa là nó phân tích nội dung gói tin, như HTTP, FTP, hoặc DNS.

**\*Ưu điểm**:

* Bảo mật cấp cao hơn nhờ kiểm tra nội dung chi tiết.
* Ẩn địa chỉ IP thực của người dùng để tăng cường quyền riêng tư.

**\*Hạn chế**:

* Chậm hơn các loại firewall khác vì kiểm tra chi tiết nội dung.
* Không phù hợp cho các mạng có lưu lượng lớn.

**2.Tổng kết**

Các công nghệ tường lửa không ngừng phát triển để đáp ứng với các mối đe dọa mạng ngày càng tinh vi. Lựa chọn công nghệ tường lửa phù hợp phụ thuộc vào:

* Quy mô và nhu cầu của tổ chức.
* Ngân sách triển khai.
* Mức độ bảo mật cần thiết.

**CHƯƠNG V - KẾT LUẬN**

Tường lửa ngày nay đóng một vai trò quan trọng trong việc bảo vệ mạng của một tổ chức nào đó tránh được danh sách gần như vô tận các tấn công đến từ Internet. Sự lựa chọn tường lửa cũng thường quyết định cách các vị trí từ xa kết nối với các hệ thống trung tâm để truy cập vào các tài nguyên cần thiết hoặc để thực hiện các nhiệm vụ quan trọng dễ dàng như thế nào. Tường lửa là "bức tường" nằm giữa một mạng (như là Internet) và máy tính (hoặc mạng nội bộ) mà nó bảo vệ. Mục đích an ninh chính của nó dành cho người dùng cá nhân là khóa các Tuy nhiên, tường lửa còn có thể làm nhiều hơn thế. Do nằm giữa 2 mạng (internet và mạng nội bộ), tường lửa có thể phân tích tất cả các lưu lượng vào và ra khỏi mạng và quyết định sẽ làm gì với dữ liệu vào ra đó. Tường lửa cũng có nhiều quy tắc để dựa vào đó cung cấp quyền truy cập dữ liệu vào mạng.

Tường lửa không chỉ là một dạng phần mềm (như tường lửa trên Windows), mà nó còn có thể là phần cứng chuyên dụng trong các mạng doanh nghiệp. Các tường lửa là phần cứng này giúp máy tính của các công ty có thể phân tích dữ liệu ra để đảm bảo rằng malware không thể thâm nhập vào mạng, kiểm soát hoạt động trên máy tính mà nhân viên của họ đang sử dụng. Nó cũng có thể lọc dữ liệu để chỉ cho phép một máy tính chỉ có thể lướt web, vô hiệu hóa việc truy cập vào các loại đữ liệu khác.