TÀI LIỆU ÔN MÔN CÔNG NGHỆ THÔNG TIN
TRONG XÉT TUYỂN VIÊN CHỨC BỆNH VIỆN ĐA KHOA
TỈNH TRÀ VINH NĂM 2023

1. Luật An ninh mạng số: 24/2018/QH14, *ngày 12 tháng 6 năm 2018* Điều 4. Nguyên tắc bảo vệ an ninh mạng

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.
3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.
4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.
5. Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.
6. Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.
7. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

Điều 5. Biện pháp bảo vệ an ninh mạng

1. Biện pháp bảo vệ an ninh mạng bao gồm:

a) Thẩm định an ninh mạng;
b) Đánh giá điều kiện an ninh mạng;
c) Kiểm tra an ninh mạng;
d) Giám sát an ninh mạng;
đ) Ứng phó, khắc phục sự cố an ninh mạng;
e) Đấu tranh bảo vệ an ninh mạng;
g) Sử dụng mật mã để bảo vệ thông tin mạng;
h) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

i) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

k) Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng;

l) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật;

m) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự;

n) Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

2. Chính phủ quy định trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm m và điểm n khoản 1 Điều này.

Điều 6. Bảo vệ không gian mạng quốc gia

Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.

Điều 8. Các hành vi bị nghiêm cấm về an ninh mạng

1. Sử dụng không gian mạng để thực hiện hành vi sau đây:

a) Hành vi quy định tại khoản 1 Điều 18 của Luật này;

b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

3. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng

Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

4. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.
5. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.
6. Hành vi khác vi phạm quy định của Luật này.

Điều 9. Xử lý vi phạm pháp luật về an ninh mạng

Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

Điều 22. Đấu tranh bảo vệ an ninh mạng

1. Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.
2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm:
a) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia;
b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia;
c) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;
d) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.
3. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.

2. Thông Tư Số: 54/2017/TT-BYT ngày 29 tháng 12 năm 2017 của Bộ Y tế ban hành bộ tiêu chí ứng dung công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh

Điều 4. Nguyên tắc xác định mức ứng dung công nghệ thông tin

1. Mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh được xác định theo bảng tổng hợp tiêu chí để đánh giá mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh quy định tại Phụ lục II Thông tư này.
2. Bảo đảm nguyên tắc khách quan, chính xác và trung thực.
3. Phải đạt tất cả tiêu chí ở mức đánh giá. Nếu có ít nhất 01 tiêu chí không đạt thì xếp ở mức thấp hơn liền kề.

Điều 5. Hướng dẫn việc xác định mức ứng dung công nghệ thông tin

1. Căn cứ vào quy định tại Điều 3 và Điều 4 Thông tư này, người đứng đầu cơ sở khám bệnh, chữa bệnh quyết định đầu tư theo thẩm quyền và ban hành quyết định xác định mức ứng dụng công nghệ thông tin tại cơ sở phụ trách. Trong trường hợp cần thiết, người đứng đầu cơ sở khám bệnh, chữa bệnh thành lập Hội đồng chuyên môn hoặc thuê tổ chức độc lập để tư vấn việc xác định mức ứng dụng công nghệ thông tin tại cơ sở phụ trách.

2. Quyết định xác định mức ứng dụng công nghệ thông tin của cơ sở khám bệnh, chữa bệnh phải được gửi báo cáo cơ quan quản lý cấp trên trực tiếp và gửi Cục Công nghệ thông tin - Bộ Y tế.

3. Người đứng đầu cơ sở khám bệnh, chữa bệnh chịu trách nhiệm trước pháp luật và cơ quan quản lý cấp trên về việc xác định mức ứng dụng công nghệ thông tin tại cơ sở phụ trách; có trách nhiệm xác định lại mức ứng dụng công nghệ thông tin nếu cơ quan quản lý y tế cấp trên kiểm tra phát hiện mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh chưa phù hợp với văn bản báo cáo.

3. Luật Công nghệ thông tin số: 67/2006/QH11 *ngày 29 thang 6 năm 2006* Điều 5 Chính sách của Nhà nước về ứng dụng và phát triển công nghệ thông tin

1. Ưu tiên ứng dụng và phát triển công nghệ thông tin trong chiến lược phát triển kinh tế - xã hội và sự nghiệp công nghiệp hóa, hiện đại hóa đất nước.

2. Tạo điều kiện để tổ chức, cá nhân hoạt động ứng dụng và phát triển công nghệ thông tin đáp ứng yêu cầu phát triển kinh tế - xã hội, đối ngoại, quốc phòng, an ninh; thúc đẩy công nghiệp công nghệ thông tin phát triển thành ngành kinh tế trọng điểm, đáp ứng nhu cầu thị trường nội địa và xuất khẩu.

3. Khuyến khích đầu tư cho lĩnh vực công nghệ thông tin.

4. Ưu tiên dành một khoản ngân sách nhà nước để ứng dụng công nghệ thông tin trong một số lĩnh vực thiết yếu, tạo lập nền công nghiệp công nghệ thông tin và phát triển nguồn nhân lực công nghệ thông tin.

5. Tạo điều kiện thuận lợi để phát triển cơ sở hạ tầng thông tin quốc gia.

6. Có chính sách ưu đãi để tổ chức, cá nhân có hoạt động ứng dụng và phát triển công nghệ thông tin đối với nông nghiệp; nông thôn, vùng sâu, vùng xa, biên giới, hải đảo; người dân tộc thiểu số, người tàn tật, người có hoàn cảnh khó khăn.

7. Bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân ứng dụng và phát triển công nghệ thông tin.

8. Tăng cường giao lưu và hợp tác quốc tế; khuyến khích hợp tác với tổ chức, cá nhân Việt Nam ở nước ngoài trong lĩnh vực công nghệ thông tin.

Điều 6. Nội dung quản lý nhà nước về công nghệ thông tin

1. Xây dựng, tổ chức thực hiện chiến lược, quy hoạch, kế hoạch, chính sách ứng dụng và phát triển công nghệ thông tin.

2. Xây dựng, ban hành, tuyên truyền, phổ biến, tổ chức thực hiện văn bản quy phạm pháp luật, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật trong lĩnh vực công nghệ thông tin.

3. Quản lý an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

4. Tổ chức quản lý và sử dụng tài nguyên thông tin, cơ sở dữ liệu quốc gia.

5. Quản lý và tạo điều kiện thúc đẩy công tác hợp tác quốc tế về công nghệ thông tin.

6. Quản lý, đào tạo, bồi dưỡng và phát triển nguồn nhân lực công nghệ thông tin.

7. Xây dựng cơ chế, chính sách và các quy định liên quan đến sản phẩm, dịch vụ công ích trong lĩnh vực công nghệ thông tin.

8. Xây dựng cơ chế, chính sách và các quy định về việc huy động nguồn lực công nghệ

thông tin phục vụ quốc phòng, an ninh và các trường hợp khẩn cấp quy định tại Điều 14 của Luật này.

9. Quản lý thống kê về công nghệ thông tin.

10. Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm trong lĩnh vực công nghệ thông tin.

Điều 7. Trách nhiệm quản lý nhà nước về công nghệ thông tin

1. Chính phủ thống nhất quản lý nhà nước về công nghệ thông tin.

2. Bộ Bưu chính, Viễn thông chịu trách nhiệm trước Chính phủ trong việc chủ trì, phối hợp với bộ, cơ quan ngang bộ có liên quan thực hiện quản lý nhà nước về công nghệ thông tin.

3. Bộ, cơ quan ngang bộ trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm chủ trì, phối hợp với Bộ Bưu chính, Viễn thông thực hiện quản lý nhà nước về công nghệ thông tin theo phân công của Chính phủ.

4. Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương trong phạm vi nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về công nghệ thông tin tại địa phương.

5. Việc tổ chức thực hiện ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước do Chính phủ quy định.

ĐỊNH NGHĨA VÀ PHÂN LOẠI FIREWALL

1. Định nghĩa:

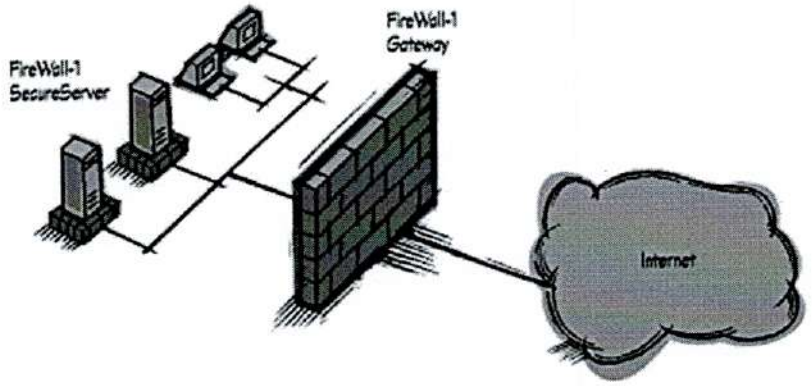
1.1. Giới thiệu về Firewall:

Firewall là một thiết bị – hay một hệ thống – điều khiển truy cập mạng, nó có thể là phần cứng hoặc phần mềm hoặc kết hợp cả hai.

Firewall thường được đặt tại mạng vành đai để đóng vai trò như cổng nối (gateway) bảo mật giữa một mạng tin cậy và mạng không tin cậy, có thể giữa Intranet và Internet hoặc giữa mạng của doanh nghiệp chủ với mạng của đối tác.

Firewall được thiết kế để ngăn chặn tất cả các lưu lượng không được phép và cho phép các lưu lượng được phép đi qua nó.

Vì thế, thiết bị firewall thường bao gồm hai giao tiếp mạng (network interface): Một nối với mạng bên trong (vd: intranet: mạng cần bảo vệ); Một nối với mạng bên ngoài (vd: Internet: mạng không tin cậy).



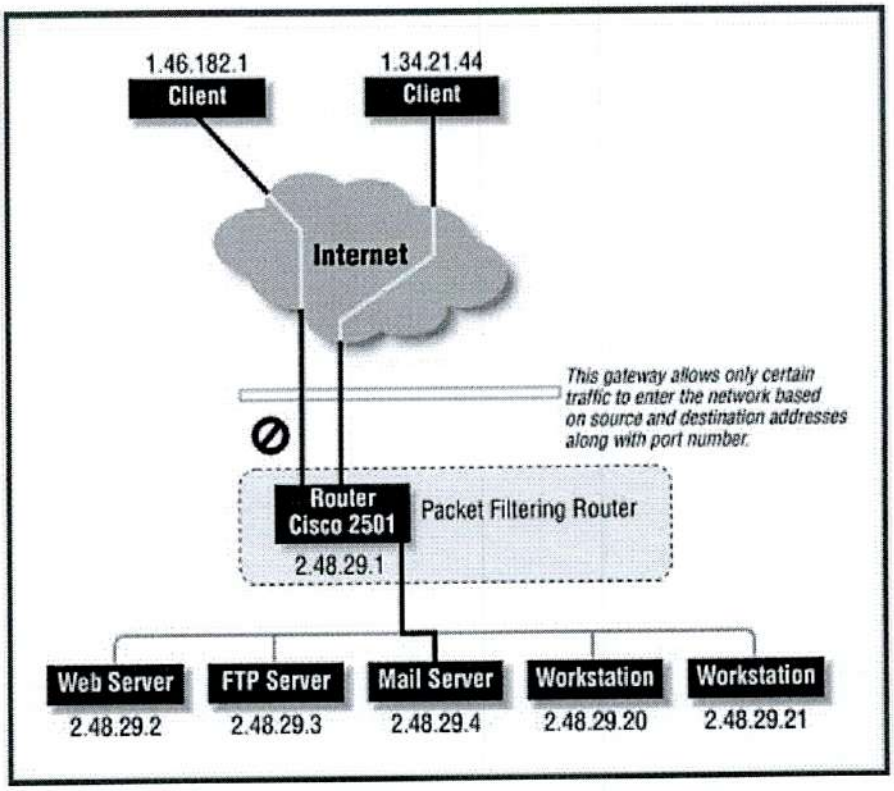
Ở đây cần phân biệt rõ, về vài trò gateway, giữa router và firewall: Như đã biết, router là thiết bị mạng, thường được sử dụng cho mục tiêu định tuyến lưu lượng mạng (có thể từ chối lưu lượng nào đó). Trong khi đó, firewall là thiết bị bảo mật, có nhiệm vụ giám sát và điều khiển lưu lượng mạng (chỉ cho phép lưu lượng thích hợp đi qua). Trong thực tế, nếu được cấu hình hợp lệ thì router có thể thực hiện một vài chức năng của firewall, nhưng điều ngược lại là khó có thể.

Ngoài ra, firewall cung cấp một cơ chế cấu hình linh hoạt hơn, nó có thể được cấu hình để cho phép/cấm (allow/deny) các lưu lượng dựa trên dịch vụ, địa chỉ IP của nguồn hoặc đích, hoặc ID của người yêu cầu sử dụng dịch vụ. Nó cũng có thể được cấu hình để ghi lại (log) tất cả các lưu lượng qua nó.

Người quản trị an ninh của hệ thống cũng có thể cấu hình để firewall thực hiện chức năng như là một trung tâm quản lý bảo mật. Tức là, firewall sẽ đóng vai trò cổng nối bảo mật tại mạng vành đai của mạng Tổ chức. Khi đó mọi lưu lượng từ bên ngoài muốn đến tất cả các hệ thống trong phạm vi mạng của một Tổ chức đều phải thông qua firewall.

1.2. Mục tiêu thiết kế một firewall:

- Tất cả lưu lượng từ mạng bên trong ra bên ngoài hoặc ngược lại phải đi qua firewall. Để đạt được mục tiêu này ta phải khóa tất cả "con đường" vào mạng bên trong, ngoại trừ thông qua firewall.
- Chỉ có lưu lượng được cho phép, được định nghĩa bởi chính sách bảo mật cục bộ (local security policy), mới được phép đi qua firewall. Nhiều loại firewall khác nhau có thể được sử dụng để cài đặt các loại chính sách bảo mật khác nhau.
- Bản thân firewall phải có khả năng tránh được sự xâm nhập bất hợp pháp. Để đạt được mục tiêu này cần phải thiết kế một hệ thống tin cậy.



*Người quản trị an ninh hệ thống phải luôn hoàn thiện các đặc tính và cấu hình hệ thống, điều này giúp loại bỏ một số rủi ro có thể xảy ra với hệ thống. Nếu hệ thống không được cấu hình hợp lệ thì sẽ tạo điều kiện cho hacker tấn công vào mạng thông qua các*dịch vụ không hợp lệ đó.

1.3. Đặc tính của Firewall:

Sau đây là các kỹ thuật chung nhất mà các firewall sử dụng để điều khiển truy cập và làm cho chính sách bảo mật của site có hiệu lực. Trước đây firewall chỉ tập trung vào điều khiển dịch vụ, nhưng hiện nay chúng có thể thực hiện bốn chức năng cụ thể sau:

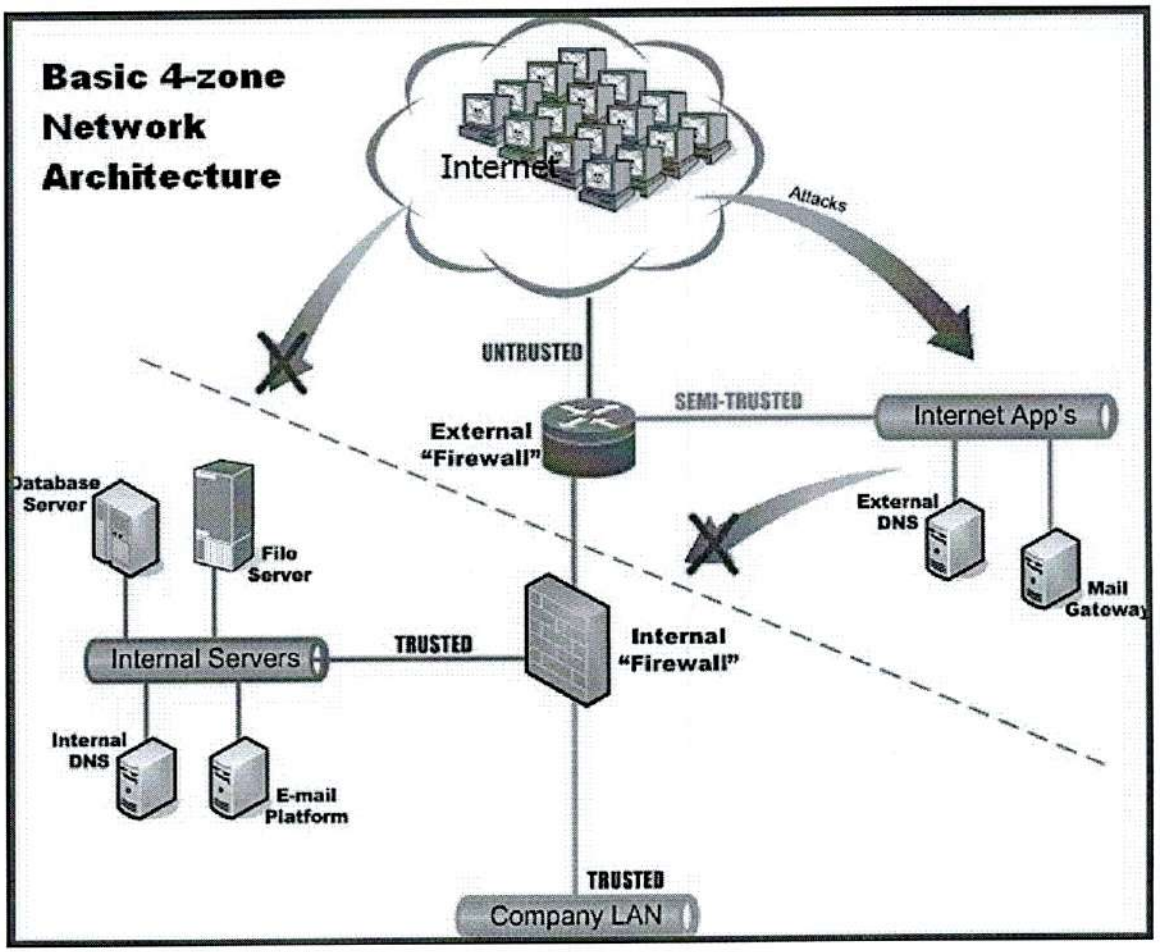
- Điều khiển dịch vụ (service control): Xác định các loại dịch vụ Internet có thể được truy cập, đi ra hoặc đi vào. Firewall có thể lọc lưu lượng dựa vào địa chỉ IP và số hiệu cổng TCP; Có thể cung cấp phần mềm proxy, mà có thể tiếp nhận và phiên dịch mỗi yêu cầu dịch vụ trước khi chuyển tiếp nó; Hoặc tự nó quản lý các phần mềm server như các dịch vụ Web hoặc Mail.
- Điều khiển hướng (direction control): Xác định hướng mà mỗi dịch vụ cụ thể yêu cầu, là có thể được khởi tạo và được phép thông qua firewall.

- Điều khiển người sử dụng (user control): Điều khiển truy cập đến một dịch vụ, mà người sử dụng đang cố gắng truy cập đến nó. Đặc trưng này thường được áp dụng cho những người sử dụng bên trong firewall vành đai (người sử dụng cục bộ). Nó cũng có thể được áp dụng cho lưu lượng đi vào, từ những người sử dụng bên ngoài.
- Điề khiển hành vi (Behaviour Control): Điều khiển các dịch vụ đặc biệt được sử dụng như thế nào. Ví dụ: firewall có thể lọc e-mail để hạn chế thư rác, hoặc nó có thể cho phép truy cập bên ngoài đến duy nhất một phần thông tin trên một server Web cục bộ.

1.4. Thuận lợi và hạn chế của Firewall:

Thuận lợi:

- Firewall định nghĩa một "choke point" đơn, làm cho người sử dụng bất hợp pháp không tiếp cận được mạng được bảo vệ, giúp bảo vệ mạng chống lại các tấn công theo kiểu spoofing IP và routing IP. Việc sử dụng "choke point" đơn làm cho việc quản lý bảo mật trở nên đơn giản hơn, vì những khả năng bảo mật được kết hợp trên một hệ thống đơn hoặc một tập các hệ thống.
- Firewall cung cấp một vị trí để giám sát các sự kiện liên quan đến bảo mật. Việc kiểm toán (audit) và cảnh báo (alarm) cũng có thể được cài đặt trên hệ thống firewall.
- Firewall là một hệ nền tiện lợi cho nhiều chức năng Internet không liên quan đến bảo mật, bao gồm, chức năng NAT (network address translator): ánh xạ địa chỉ mạng cục bộ thành địa chỉ Internet, và chức năng quản trị mạng: kiểm toán và ghi lại các thông tin liên quan đến việc sử dụng Internet.
- Firewall có thể phục vụ như là một hệ nền cho IPSec. Khi chế độ đường hầm được triển khai, firewall có thể được sử dụng để cài đặt các mạng riêng ảo.



Hạn chế:

- Firewall không thể bảo vệ để chống lại các tấn công không đi qua firewall. Các hệ thống nội bộ có thể có khả năng dial-out để kết nối với một ISP. Một LAN nội bộ có thể hỗ trợ một modem pool, mà nó cung cấp khả năng dial-in cho nhân viên lưu động.
- Firewall không thể chống lại các nguy cơ tấn công từ chính bên trong mạng nội bộ mà nó bảo vệ, nhất là khi có một người sử dụng từ bên trong hợp tác với kẻ tấn công bên ngoài.
- Firewall không thể bảo vệ chống lại việc chuyển các chương trình hoặc file có virus đi qua nó.

2. Phân loại ffirewall:

FIREWALL TẦNG ỨNG DỤNG & FIREWALL LỌC GÓI:

Nếu dựa vào nguyên lý hoạt động của firewall thì ta có thể chia nó thành hai loại chính: Firewall tầng ứng dụng và Firewall lọc gói tin.

Mặc dầu hoạt động theo hai nguyên lý khác nhau, nhưng với cấu hình phù hợp thì cả hai đều có thể thực hiện các chức năng bảo mật mạng, bằng việc ngăn chặn lưu lượng/gói tin không được phép đi qua nó.

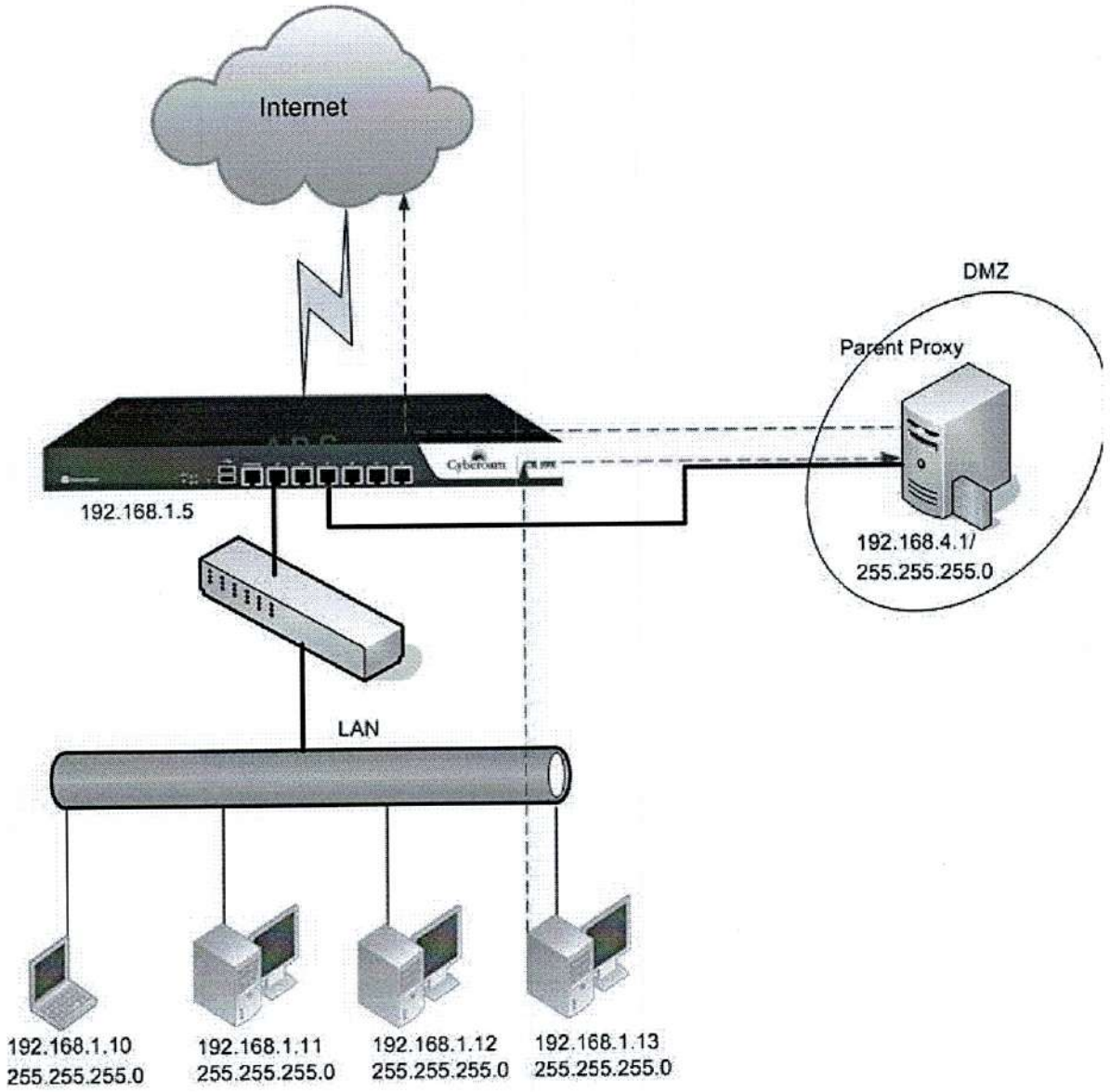
Ngoài ra, có thể xem: Circuite-level Gateway; Stateful Inspection Firewall; Bastion Host là một trong các loại firewall khác.

Sau đây chúng ta sẽ xem xét, làm thế nào để các chính sách bảo mật có hiệu lực trên các loại firewall này.

Firewall tầng ứng dụng (Application Level firewalls)

Firewall tầng ứng dụng, cũng có thể gọi là Proxy, là các gói phần mềm hoạt động trên các hệ điều hành đa năng – như hệ điều hành Windown NT hoặc Unix, hoặc trên các thiết bị firewall.

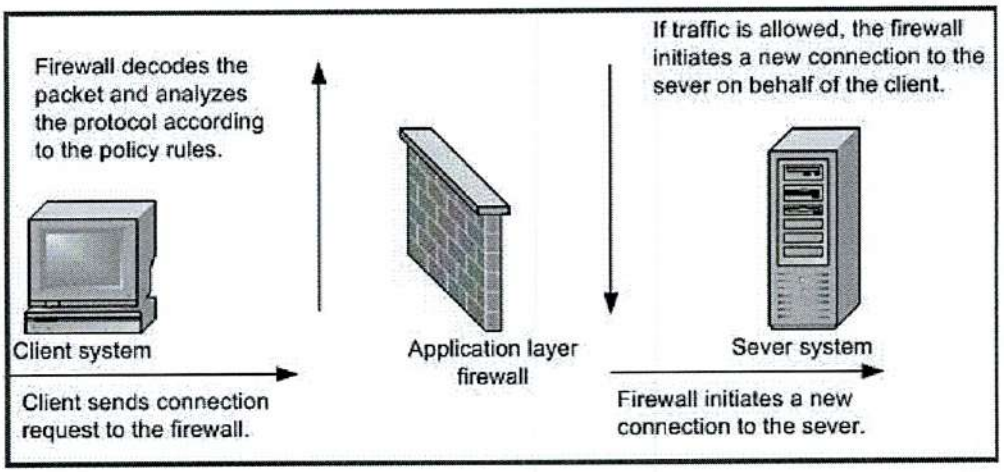
Loại này có thể có nhiều giao diện (interface) mạng – ít nhất là 2 giao diện, mỗi giao diện được dùng để nối với một mạng được kết nối với nó. Một tập các luật chính sách được định nghĩa, để chỉ ra lưu lượng nào là được phép chuyển từ mạng này sang các mạng khác – hay từ giao diện này qua giao diện khác. Nếu một luật chỉ ra là không cho phép lưu lượng đi qua, thì firewall sẽ từ chối hoặc hủy bỏ các gói tin trong lưu lượng đó .



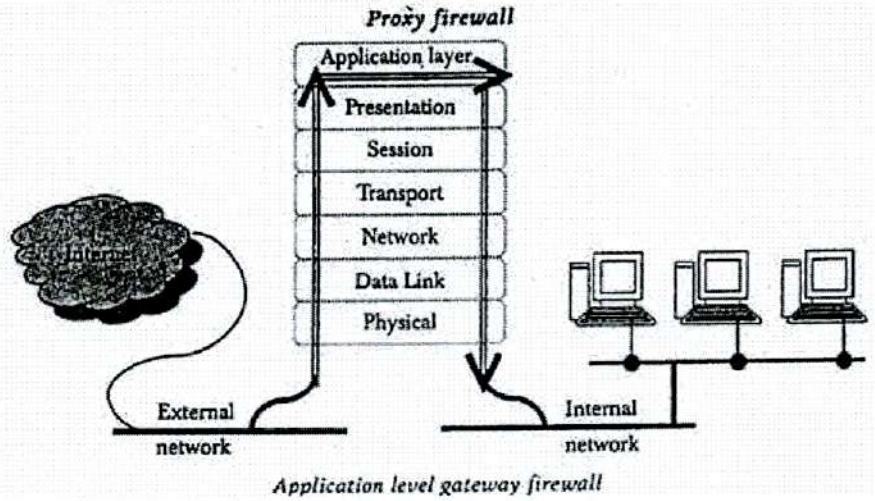
Tập luật chính sách sẽ có hiệu lực thông qua việc sử dụng các proxy trên firewall. Trên các firewall tầng ứng dụng, mỗi giao thức "được phép" phải có một proxy riêng của nó.

Một proxy tốt là một proxy được xây dựng một cách cụ thể cho một giao thức cụ thể. Ví dụ, proxy FTP hiểu giao thức FTP và chỉ có thể quyết định, cho phép đi qua hoặc bị chặn lại, với các lưu lượng được mang bởi giao thức này, tất nhiên là phải dựa trên các tập luật chính sách đã được định nghĩa.

Với firewall tầng ứng dụng, tất cả các kết nối đều kết thúc trên firewall. Xem hình sau:



Hình này cho thấy, một kết nối bắt đầu ở hệ thống Client và đi tới giao diện bên trong của firewall. Firewall chấp nhận kết nối này, phân tích nội dung của gói và giao thức được sử dụng, và nếu tập luật chính sách cho phép lưu lượng đi qua thì firewall sẽ khởi tạo một kết nối mới từ giao diện bên ngoài của nó đến hệ thống Server.



Application level gateway firewall

Firewall tầng ứng dụng cũng sử dụng các proxy để kiểm soát các kết nối đi vào. Trong trường hợp này, proxy trên firewall sẽ nhận các kết nối đi vào và thực hiện các xử lý cần thiết trước khi lưu lượng được gửi tới hệ thống đích. Nhờ đó mà firewall có thể bảo vệ hệ thống mạng bên trong, ngăn chặn các tấn công được khởi tạo thông qua các ứng dụng.

Đa số các Firewall tầng ứng dụng đều thiết kế các proxy cho các giao thức thường được sử dụng trong các dịch vụ Internet hiện nay, như là HTTP, SMTP, FTP,Telnet,... Theo đó, chỉ những gói tin được mang bởi các giao thức này mới được xem xét, được đi qua hay bị chặn lại, qua khi đi qua Proxy. Tất nhiên, các gói tin được mang bởi các giao thức khác sẽ không được đi qua Proxy này.

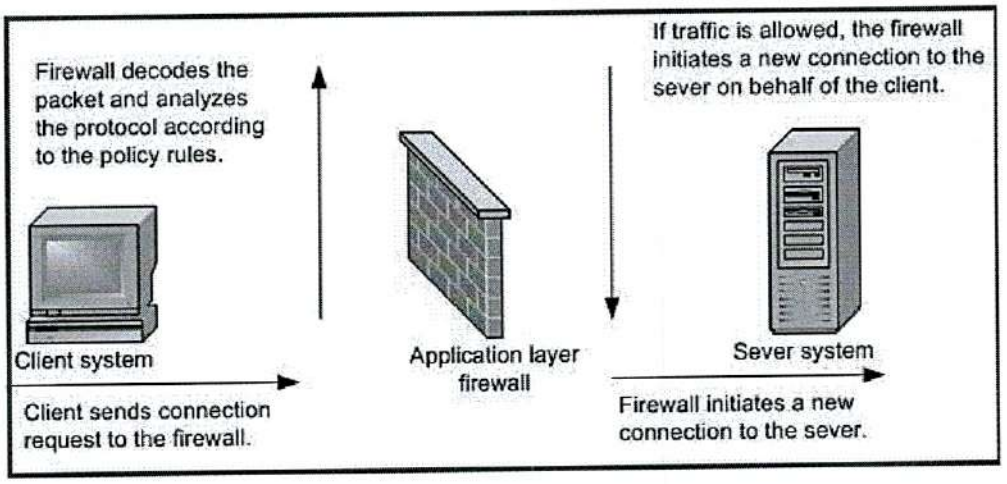
Firewall tầng ứng dụng cũng "ẩn" địa chỉ IP của các hệ thống phía sau nó. Bởi vì, tất cả kết nối đều khởi tạo và kết thúc trên các giao diện của firewall, các hệ thống bên trong (internal) không "hiện" trực tiếp ra bên ngoài và nhờ đó mà lược đồ địa chỉ IP của mạng bên trong được "ẩn" với thế giới Internet bên ngoài.

Firewall lọc gói (IP Packet Filter Firewalls)

Firewall lọc gói (tin) cũng có thể là các gói phần mềm hoạt động trên các hệ điều hành đa năng – như Windows NT hoặc Unix, hoặc trên các thiết bị firewall.

Firewall loại này có thể có nhiều giao diện mạng – ít nhất là hai giao diện, mỗi giao diện được dùng để nối với một mạng được kết nối với nó. Cũng như các firewall tầng ứng dụng, một tập các luật chính sách được định nghĩa, chỉ ra lưu lượng nào là được phép chuyển từ mạng này sang các mạng khác nào đó. Nếu một luật chỉ ra là không cho phép lưu lượng đi qua, thì firewall sẽ từ chối hoặc hủy bỏ các gói tin trong lưu lượng đó .

Với Firewall lọc gói, các kết nối không kết thúc trên firewall, xem hình sau, nó đi trực tiếp đến hệ thống đích. Khi các gói tin được gửi đến firewall, firewall sẽ kiểm tra xem gói và trạng thái kết nối có được cho phép bởi các luật chính sách đã được định nghĩa hay không. Nếu được phép, gói tin sẽ được gửi đi theo đúng hướng truyền của nó. Nếu không, thì gói sẽ bị từ chối hoặc bị hủy bỏ.



Các firewall lọc gói không dựa vào proxy cho mỗi giao thức, vì thế nó có thể được sử dụng với bất kỳ giao thức nào chạy trên IP. Một số giao thức yêu cầu firewall phải hiểu được chúng đang làm gì.

Ví dụ, FPT sử dụng một kết nối cho khởi tạo logon và một số lệnh nào đó, trong khi một kết nối khác được sử dụng để truyền các file. Kết nối được sử dụng để truyền file được xem như là một phần của kết nối FTP và vì thế firewall phải có khả năng đọc lưu lượng và hiểu các cổng kết nối mới sẽ được sử dụng. Nếu firewall không thể làm được điều này, chuyển giao file sẽ thất bại.

Chú ý: Một cách tương đối: các firewall lọc gói có khả năng xử lý một lượng lưu lượng lớn hơn các firewall ứng dụng.

Firewall lọc gói hoàn toàn không sử dụng các proxy, tức là lưu lượng từ Client được gửi truyền trực tiếp đến Server. Trong trường hợp này, nếu một hacker thực hiện cuộc tấn công chống lại Server trên một dịch vụ mở nào đó, mà dịch vụ này được cho phép bởi các luật chính sách firewall, thì firewall sẽ không cản trở hacker. Firewall lọc gói cũng có thể cho phép lược đồ địa chỉ bên trong được nhìn thấy từ bên ngoài. Địa chỉ bên trong không cần ẩn vì các kết nối không kết thúc trên firewall.

Các luật chính sách có hiệu lực khi sử dụng các bộ lọc kiểm tra gói. Các bộ lọc sẽ kiểm tra các gói và quyết định lưu lượng có được phép đi qua hay không, dựa trên các luật chính sách và trạng thái kết nối hiện tại của giao thức.

Người biên soạn	**PHÊ DUYỆT**
	SỞ Y TẾ TỈNH ... BỆNH VIỆN ĐA KHOA ...
KS. Diệp Văn Út	**TS.BS Trần Kiến Vũ**