Thực hành Xây dựng một Mail Server - Thực hành Proxy và Firewall

Bởi:

Khoa CNTT ĐHSP KT Hưng Yên

Thực hành Xây dựng một Mail Server

Chuẩn bị

Một Server đã cài dịch vụ DNS, IIS

Mail Server Mdeamon hoặc Exchange

Yêu cầu:

Cấu hình mail Server và tạo account cho các thành viên trong lớp sử dụng để gửi và nhận mail

Thực hành Proxy và Firewall

Nguyên lý hoạt động của Proxy

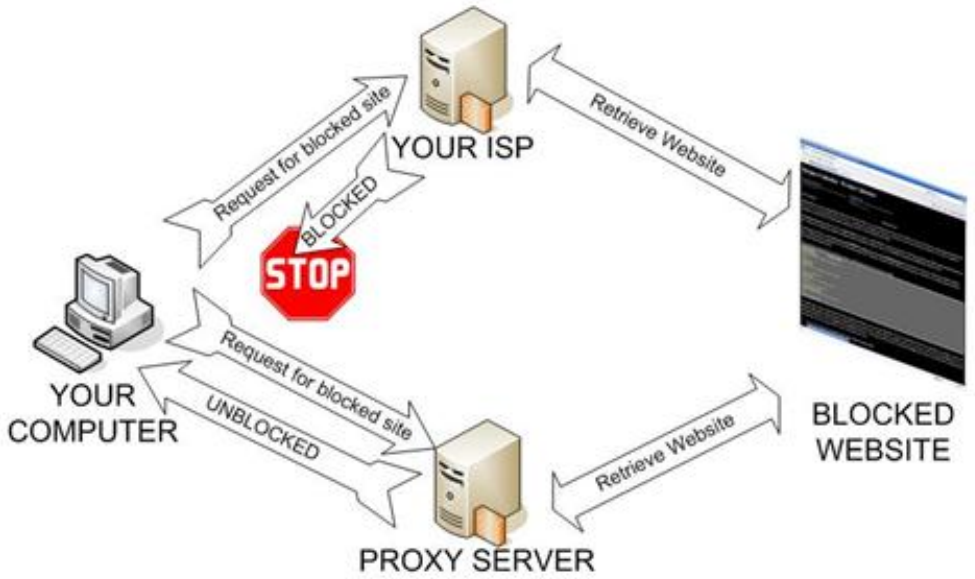
Khái niệm Proxy

Proxy là một Internet server làm nhiệm vụ chuyển tiếp thông tin và kiểm soát tạo sự an toàn cho việc truy cập Internet của các máy khách, còn gọi là khách hàng sử dụng dịch vụ internet. Trạm cài đặt proxy gọi là proxy server. Proxy hay trạm cài đặt proxy có địa chỉ IP và một cổng truy cập cố định. Ví dụ: 123.234.111.222:80 Địa chỉ IP của proxy trong ví dụ là 123.234.111.222 và cổng truy cập là 80.

Chức năng của proxy

Đối với một só hãng, công ty người ta sử dụng proxy vào việc:

-Proxy chia sẽ đường truyền: giúp nhiều máy truy cập Internet thông qua 1 máy, mà máy này gọi là Proxy server. Chỉ duy nhất máy Proxy này cần modem và account truy cập internet, các máy client (các máy trực thuộc) muốn truy cập internet qua máy này chỉ cần nối mạng LAN tới máy Proxy và truy cập địa chỉ yêu cầu.Những yêu cầu của người sử dung sẽ qua trung gian proxy server thay thế cho server thật sự mà người sử dụng cần giao tiếp, tại điểm trung gian này công ty kiểm soát được mọi giao tiếp từ trong công ty ra ngoài intrnet và từ internet vào máy của công ty. Sử dụng Proxy, công ty có thể cấm nhân viên truy cập những địa chỉ web không cho phép, cải thiện tốc độ truy cập nhờ sự lưu trữ cục bộ các trang web trong bộ nhớ của proxy server và giấu định danh địa chỉ của mạng nội bộ gây khó khăn cho việc thâm nhập từ bên ngoài vào các máy của công ty.



Đối với các nhà cung cấp dịch vụ đường truyền internet:

-Do trên mạng internet có lượng thông tin rất phong phú, theo quan điểm của từng quốc gia, của từng chủng tộc hay địa phương, các nhà cung cấp dịch vụ internet khu vực đó sẽ phối hợp proxy với kỹ thuật tường lửa để tạo ra một bộ lọc gọi là firewall proxy nhằm ngăn chặn các thông tin độc hại hoặc trái thuần phong mỹ tục đối với quốc gia, đói với chủng tộc hay địa phương đó. Địa chỉ các websit mà khách hàng yêu cầu truy cập sẽ được lọc tại bộ lọc này, nếu địa chỉ không bị cấm thì yêu cầu của khách hàng tiếp tục được gửi đi, tới các DNS server của các nhà cung cấp dịch vụ. Firewall proxy sẽ lọc tất cả các thông tin từ internet gửi vào máy của khách hàng và ngược lại.

Ý nghĩa của proxy

Proxy không chỉ có giá trị bởi nó làm được nhiệm vụ của một bộ lọc thông tin, nó còn tạo ra được sự an toàn cho các khách hàng của nó, firewal Proxy ngăn chặn hiệu quảt sư xâm nhập của các đối tượng không mong muốn vào máy của khách hàng. Proxy lưu trữ

được các thông tin mà khách hàng cần trong bộ nhớ, do đó làm giảm thời gian truy tìm làm cho việc sử dụng băng thông hiệu quả.

Proxy server giống như một vệ sĩ bảo vệ khỏi những rắc rối trên Internet. Một Ps thường nằm bên trong tường lửa, giữa trình duyệt web và server thật, làm chức năng tạm giữ những yêu cầu Internet của các máy khách để chúng không giao tiếp trực tiếp Internet. Người dùng sẽ không truy cập được những trang web không cho phép (bị công ty cấm).

Mọi yêu cầu của máy khách phải qua Ps, nếu địa chỉ IP có trên proxy, nghĩa là Website này được lưu trữ cục bộ, thì trang này sẽ đươc truy cập mà không cần phải kết nối Internet, nếu không có trên Ps và trang này không bị cấm yêu cầu sẽ được chuyển đến server thật, DNS server... và ra Internet. Ps lưu trữ cục bộ các trang Web thường truy cập nhất trong bộ đệm giảm chi phí, tốc độ hiển thị trang Web nhanh.

Proxy server bảo vệ mạng nội bộ khỏi bị xác định bởi bên ngoài bằng cách mang lại cho mạng hai định danh: một cho nội bộ, một cho bên ngoài. Điều này tạo ra một "bí danh" đối với thế giới bên ngoài gây khó khăn đối với nếu người dùng "tự tung tự tác" hay các tay bẻ khóa muốn xâm nhập trực tiếp máy nào đó.

Cách sử dụng proxy hiệu quả

Do các proxy có quy mô bộ nhớ khác nhau và số lượng người đang sử dụng proxy nhiều-ít khác nhau, Proxy server hoạt động quá tải thì tốc độ truy cập internet của khách hàng có thể bị chậm. Mặt khác một số websit khách hàng có đầy đủ điều kiện nhân thân để đọc, nghiên cứu nhưng bị tường lửa chặn không truy cập được thì biện pháp đổi proxy để truy cập là điều cần thiết nhằm đảm bảo công việc. Do đó người sử dụng có thể chọn proxy server để sử dụng cho riêng mình. Có các cách chọn lựa cho người sử dụng. Sử dụng proxy mặc định của nhà cung cấp dịch vụ (internet), trường hợp này người sử dụng không cần điền địa chỉ IP của proxy vào cửa sổ internet option của trình duyệt trong máy của mình. Sử dụng proxy server khác (phải trả phí hoặc miễn phí) thì phải điền địa chỉ IP của proxy server vào cửa sổ internet option của trình duyệt.

Một số Proxy miễn phí tham khảo

IP address	Anonymity level	Checked time	Country
203.252.226.215:8001	transparent	Dec-26, 18:26	Korea, Republic of
81.20.173.65:3128	transparent server	Dec-26, 10:08	Russian Federation
81.92.147.62:3128	transparent	Dec-26, 18:15	Czech Republic
189.15.68.99:3128	transparent	Dec-26, 16:14	Brazil
141.223.175.140:8080	transparent proxy server	Dec-26, 15:57	Korea, Republic of
85.226.20.158:3128	transparent proxy	Dec-26, 14:49	Sweden
66.29.36.95:554	hight-anonymous ($)	Dec-27, 06:01	United States
88.243.48.144:3128	transparent	Dec-26, 18:22	Turkey
213.144.14.66:3128	transparent server	Dec-26, 20:44	Germany
212.62.102.247:80	transparent proxy	Dec-26, 14:43	Saudi Arabia
61.19.237.202:8080	transparent	Dec-26, 09:55	Thailand
61.50.217.230:1080	transparent proxy	Dec-26, 09:55	China
202.206.100.39:3128	transparent proxy	Dec-26, 15:59	China
61.142.249.116:8080	transparent proxy	Dec-26, 09:59	China
118.98.212.242:3128	transparent proxy	Dec-26, 19:05	Indonesia
203.73.180.16:3128	transparent	Dec-25, 18:26	Taiwan
200.129.25.3:8080	transparent proxy	Dec-26, 18:29	Brazil
203.190.51.206:8080	transparent server	Dec-25, 14:21	Indonesia
212.62.102.134:80	transparent server	Dec-25, 14:23	Saudi Arabia

Nguyên lý hoạt động của Firewall

Khái niệm tường lửa (Firewall)

Trong ngành mạng máy tính, bức tường lửa (tiếng Anh: firewall) là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

Tường lửa là một thiết bị phần cứng và/hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các tòa nhà. Tường lửa còn được gọi là Thiết bị bảo vệ biên giới (Border Protection Device - BPD), đặc biệt trong các ngữ cảnh của NATO, hay bộ lọc gói tin (packet filter) trong hệ điều hành BSD - một phiên bản Unix của Đại học California, Berkeley.

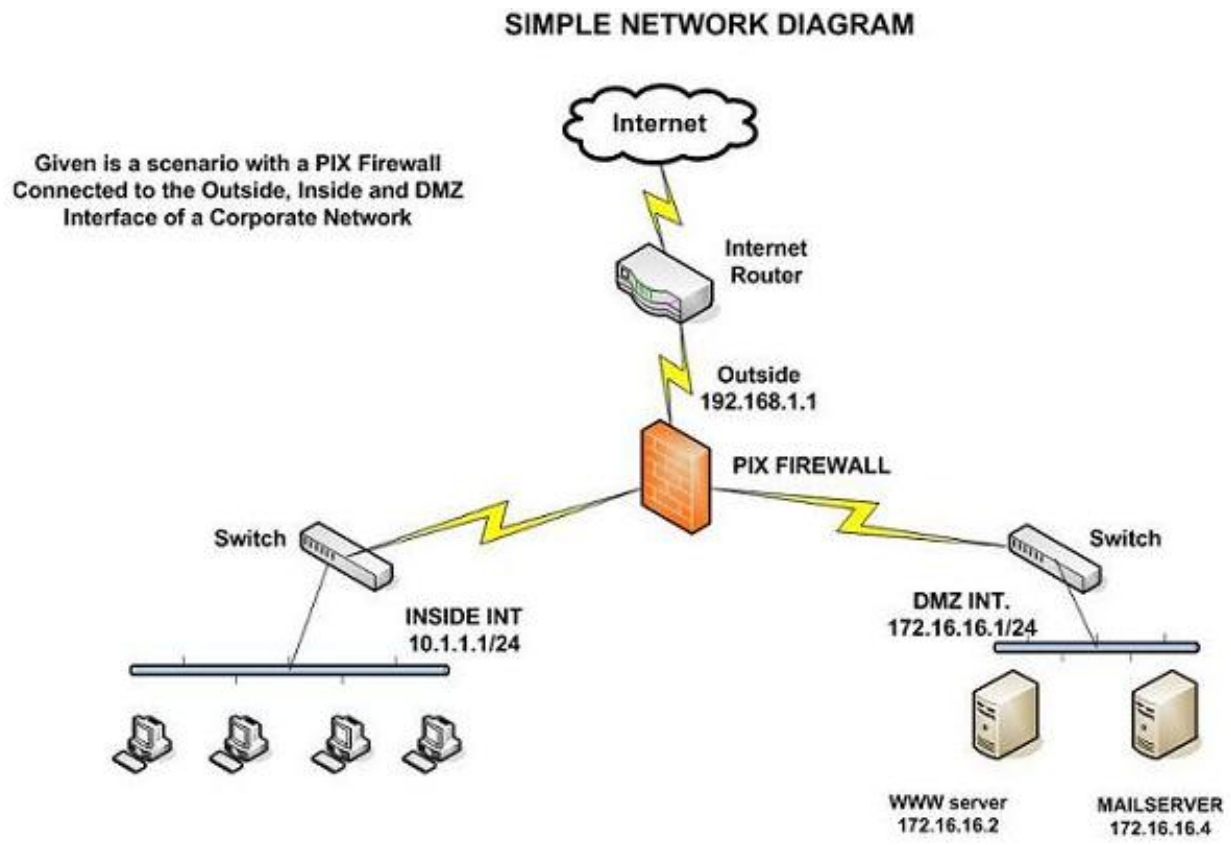
Nhiệm vụ cơ bản của tường lửa là kiểm soát giao thông dữ liệu giữa hai vùng tin cậy khác nhau. Các vùng tin cậy (zone of trust) điển hình bao gồm: mạng Internet (vùng

không đáng tin cậy) và mạng nội bộ (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc quyền tối thiểu (principle of least privilege).

Cấu hình đúng đắn cho các tường lửa đòi hỏi kĩ năng của người quản trị hệ thống. Việc này đòi hỏi hiểu biết đáng kể về các giao thức mạng và về an ninh máy tính. Những lỗi nhỏ có thể biến tường lửa thành một công cụ an ninh vô dụng.

Lịch sử phát triển Firewall

Công nghệ tường lửa bắt đầu xuất hiện vào cuối những năm 1980 khi Internet vẫn còn là một công nghệ khá mới mẻ theo khía cạnh kết nối và sử dụng trên toàn cầu. Ý tưởng đầu tiên được đã hình thành sau khi hàng loạt các vụ xâm phạm nghiêm trọng đối với an ninh liên mạng xảy ra vào cuối những năm 1980. Năm 1988, một nhân viên tại trung tâm nghiên cứu NASA Ames tại California gửi một bản ghi nhớ qua thư điện tử tới đồng nghiệp rằng: "Chúng ta đang bị một con VIRUS Internet tấn công! Nó đã đánh Berkeley, UC San Diego, Lawrence Livermore, Stanford, và NASA Ames." Con virus được biết đến với tên Sâu Morris này đã được phát tán qua thư điện tử và khi đó đã là một sự khó chịu chung ngay cả đối với những người dùng vô thưởng vô phạt nhất. Sâu Morris là cuộc tấn công diện rộng đầu tiên đối với an ninh Internet. Cộng đồng mạng đã không hề chuẩn bị cho một cuộc tấn công như vậy và đã hoàn toàn bị bất ngờ. Sau đó, cộng đồng Internet đã quyết định rằng ưu tiên tối cao là phải ngăn chặn không cho một cuộc tấn công bất kỳ nào nữa có thể xảy ra, họ bắt đầu cộng tác đưa ra các ý tưởng mới, những hệ thống và phần mềm mới để làm cho mạng Internet có thể trở lại an toàn.



Năm 1988, bài báo đầu tiên về công nghệ tường lửa được công bố, khi Jeff Mogul thuộc Digital Equipment Corp. phát triển các hệ thống lọc đầu tiên được biết đến với tên các tường lửa lọc gói tin. Hệ thống khá cơ bản này đã là thế hệ đầu tiên của cái mà sau này sẽ trở thành một tính năng kỹ thuật an toàn mạng được phát triển cao. Từ năm 1980 đến năm 1990, hai nhà nghiên cứu tại phòng thí nghiệm AT&T Bell, Dave Presetto và Howard Trickey, đã phát triển thế hệ tường lửa thứ hai, được biến đến với tên các tường lửa tầng mạch (circuit level firewall). Các bài báo của Gene Spafford ở Đại học Purdue, Bill Cheswick ở phòng thí nghiệm AT&T và Marcus Ranum đã mô tả thế hệ tường lửa thứ ba, với tên gọi tường lửa tầng ứng dụng (application layer firewall), hay tường lửa dựa proxy (proxy-based firewall). Nghiên cứu công nghệ của Marcus Ranum đã khởi đầu cho việc tạo ra sản phẩn thương mại đầu tiên. Sản phẩm này đã được Digital Equipment Corporation's (DEC) phát hành với tên SEAL. Đợt bán hàng lớn đầu tiên của DEC là vào ngày 13 tháng 9 năm 1991 cho một công ty hóa chất tại bờ biển phía Đông của Mỹ.

Tại AT&T, Bill Cheswick và Steve Bellovin tiếp tục nghiên cứu của họ về lọc gói tin và đã phát triển một mô hình chạy được cho công ty của chính họ, dựa trên kiến trúc của thế hệ tường lửa thứ nhất của mình. Năm 1992, Bob Braden và Annette DeSchon tại Đại học Nam California đã phát triển hệ thống tường lửa lọc gói tin thế hệ thứ tư. Sản phẩm có tên “Visas” này là hệ thống đầu tiên có một giao diện với màu sắc và các biểu tượng, có thể dễ dàng cài đặt thành phần mềm cho các hệ điều hành chẳng hạn Microsoft

Windows và Mac/OS của Apple và truy nhập từ các hệ điều hành đó. Năm 1994, một công ty Israel có tên Check Point Software Technologies đã xây dựng sản phẩm này thành một phần mềm sẵn sàng cho sử dụng, đó là FireWall-1. Một thế hệ thứ hai của các tường lửa proxy đã được dựa trên công nghệ Kernel Proxy. Thiết kế này liên tục được cải tiến nhưng các tính năng và mã chương trình cơ bản hiện đang được sử dụng rộng rãi trong cả các hệ thống máy tính gia đình và thương mại. Cisco, một trong những công ty an ninh mạng lớn nhất trên thế giới đã phát hành sản phẩm này năm 1997.

Thế hệ FireWall-1 mới tạo thêm hiệu lực cho động cơ kiểm tra sâu gói tin bằng cách chia sẻ chức năng này với một hệ thống ngăn chặn xâm nhập.

Các loại tường lửa

Có ba loại tường lửa cơ bản tùy theo:

- Truyền thông được thực hiện giữa một nút đơn và mạng, hay giữa một số mạng.
- Truyền thông được chặn tại tầng mạng, hay tại tầng ứng dụng.
- Tường lửa có theo dõi trạng thái của truyền thông hay không.

Phân loại theo phạm vi của các truyền trông được lọc, có các loại sau:

- Tường lửa cá nhân, một ứng dụng phần mềm với chức năng thông thường là lọc dữ liệu ra vào một máy tính đơn.
- Tường lửa mạng, thường chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các khu phi quân sự (mạng con trung gian nằm giữa mạng nội bộ và mạng bên ngoài). Một tường lửa thuộc loại này lọc tất cả giao thông dữ liệu vào hoặc ra các mạng được kết nối qua nó.

Loại tường lửa mạng tương ứng với ý nghĩa truyền thống của thuật ngữ "tường lửa" trong ngành mạng máy tính.

Khi phân loại theo các tầng giao thức nơi giao thông dữ liệu có thể bị chặn, có ba loại tường lửa chính:

- Tường lửa tầng mạng. Ví dụ iptables.
- Tường lửa tầng ứng dụng. Ví dụ TCP Wrappers.
- Tường lửa ứng dụng. Ví dụ: hạn chế các dịch vụ ftp bằng việc định cấu hình tại tệp /etc/ftpaccess.

Các loại tường lửa tầng mạng và tường lửa tầng ứng dụng thường trùm lên nhau, mặc dù tường lửa cá nhân không phục vụ mạng, nhưng một số hệ thống đơn đã cài đặt chung cả hai.

Cuối cùng, nếu phân loại theo tiêu chí rằng tường lửa theo dõi trạng thái của các kết nối mạng hay chỉ quan tâm đến từng gói tin một cách riêng rẽ, có hai loại tường lửa:

- Tường lửa có trạng thái (Stateful firewall)
- Tường lửa phi trạng thái (Stateless firewall)

Lý do sử dụng tường lửa

Mạng internet ngày càng phát triển và phổ biến rộng khắp mọi nơi, lợi ích của nó rất lớn. Tuy nhiên cũng có rất nhiều ngoại tác không mong muốn đối với các cá nhân là cha mẹ hay tổ chức, doanh nghiệp, cơ quan nhà nước... như các trang web không phù hợp lứa tuổi, nhiệm vụ, lợi ích, đạo đức, pháp luật hoặc trao đổi thông tin bất lợi cho cá nhân, doanh nghiệp... Do vậy họ (các cá nhân, tổ chức, cơ quan và nhà nước) sử dụng tường lửa để ngăn chặn.

Một lý do khác là một số quốc gia theo chế độ độc tài, độc đảng áp dụng tường lửa để ngăn chặn quyền trao đổi, tiếp cận thông tin của công dân nước mình không cho họ truy cập vào các trang web hoặc trao đổi với bên ngoài, điều mà nhà cầm quyền cho rằng không có lợi cho chế độ đó.

Cách thức ngăn chặn

Để ngăn chặn các trang web không mong muốn, các trao đổi thông tin không mong muốn người ta dùng cách lọc các địa chỉ web không mong muốn mà họ đã tập hợp được hoặc lọc nội dung thông tin trong các trang thông qua các từ khóa để ngăn chặn những người dùng không mong muốn truy cập vào mạng và cho phép người dùng hợp lệ thực hiện việc truy xuất.

Bức tường lửa có thể là một thiết bị định hướng (Router, một thiết bị kết nối giữa hai hay nhiều mạng và chuyển các thông tin giữa các mạng này) hay trên một máy chủ (Server), bao gồm phần cứng và/hoặc phần mềm nằm giữa hai mạng (chẳng hạn mạng Internet và mạng liên kết các gia đình, điểm kinh doanh internet, tổ chức, công ty, hệ thống Ngân hàng, cơ quan nhà nước.

Cơ quan nhà nước có thể lập bức tường lửa ngay từ cổng Internet quốc gia hoặc yêu cầu các nhà cung cấp dịch vụ đường truyền (IXP) và cung cấp dịch vụ Internet (ISP) thiết lập hệ thống tường lửa hữu hiệu hoặc yêu cầu các đại lý kinh doanh internet thực hiện các biện pháp khác như Thông tư liên tịch số 02/2005/TTLT về quản lý đại lý Internet có hiệu lực vào đầu tháng 8-2005 ở Việt Nam.

Vượt tường lửa

Các trang web bị chặn nhất là các trang web sex thường rất linh động thay đổi địa chỉ để tránh sự nhận diện hoặc nhanh chóng thông báo địa chỉ mới một cách hạn chế với các đối tượng dùng đã định.

Người dùng ở các nước có hệ thống tường lửa có thể tiếp cận với nội dung bị chặn qua các ngõ khác bằng cách thay đổi địa chỉ Proxy, DNS hoặc qua vùng nhớ đệm cached của trang tìm kiếm thông dụng như Google, Yahoo..., hoặc sử dụng phần mềm miễn phí Tor. Nói chung người dùng mạng hiểu biết nhiều về máy tính thì biết nhiều kỹ xảo vượt tường lửa.

Hiệu quả khi sử dụng tường lửa

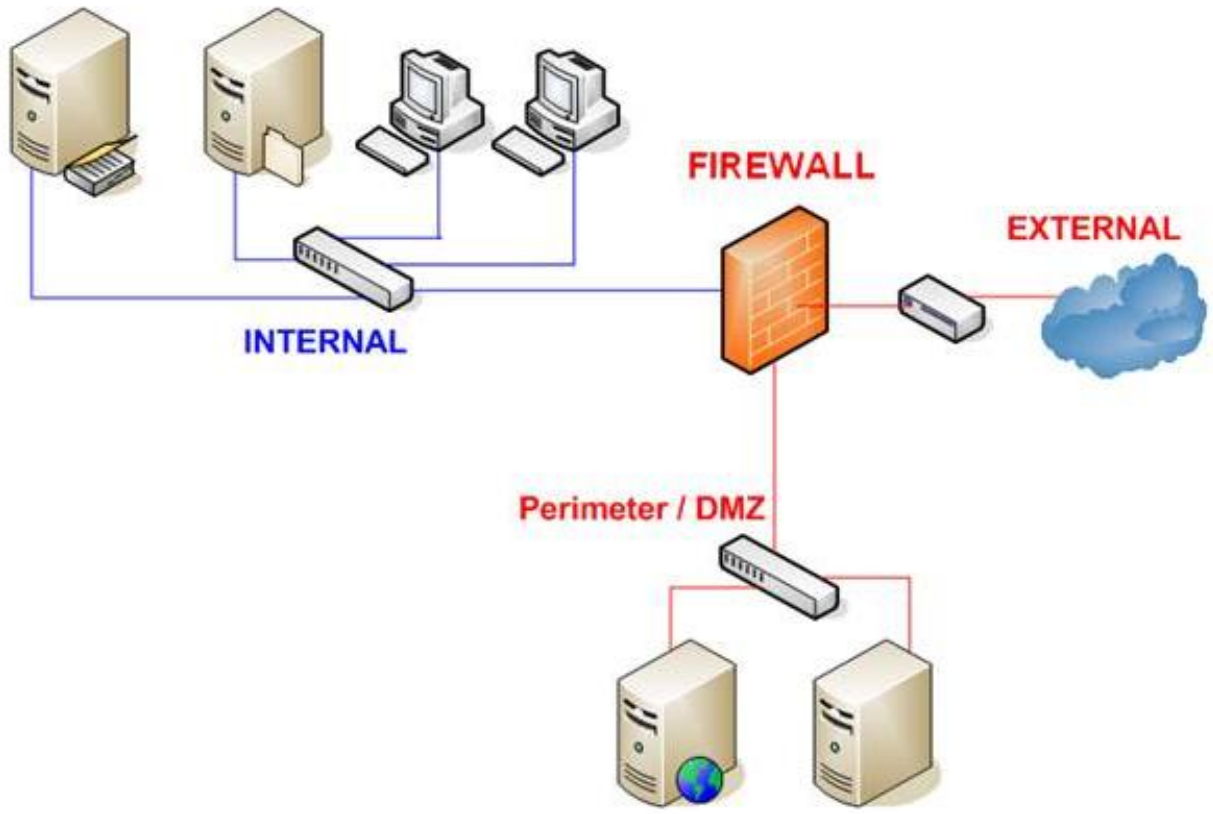
Bức tường lửa chỉ có hiệu quả tốt một thời gian sau đó các trang web bị chặn cũng như người sử dụng dùng mưu mẹo, kỹ xảo, kỹ thuật để né và vuợt tường, vì vậy phải luôn luôn cập nhật kỹ thuật, nhận điện các địa chỉ mới để thay đổi phương thức hoạt động, điều này làm tốc độ truy cập chung bị giảm và đòi hỏi phải nâng cấp trang thiết bị, kỹ thuật.

Nhược điểm khi sử dụng tường lửa

Sử dụng tường lửa cần phải xử lý một lượng lớn thông tin nên việc xử lý lọc thông tin có thể làm chậm quá trình kết nối của người kết nối.

Việc sử dụng tường lửa chỉ hữu hiệu đối với những người không thành thạo kỹ thuật vượt tường lửa, những người sử dụng khác có hiểu biết có thể dễ dàng vượt qua tường lửa bằng cách sử dụng các proxy không bị ngăn chặn.

Triển khai xây dựng hệ thống tường lửa cho doanh nghiệp



Mô tả sơ đồ hệ thống:

- Gồm 01 PC đóng vai trò Domain Controller (DC)
- Mạng LAN thuộc dải IP 192.168.1.0/24
- DMZ thuộc dải IP 172.16.1.0/24
- External có dải IP 10.0.0.0/30
- Firewall có 03 Fast Ethernet tương ứng 03 phân vùng LAN (Internal), DMZ và External

Yêu cầu:

- Các PC join vào Domain (DC)
- File Server và Web Server thuộc vùng DMZ cho phép các PC thuộc LAN truy cập vào
- Các PC thuộc LAN có thể truy cập Internet theo sự cho phép của Firewall