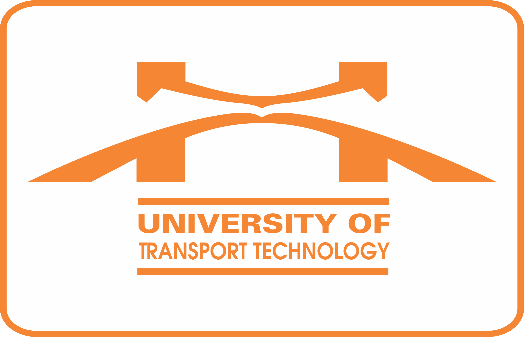
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ GIAO THÔNG

VẬN TẢI

**-----🙞🙜🕮🙞🙜-----**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO THỰC TẬP TỐT NGHIỆP**

**Ngành: CNKT ĐIỂN TỬ - VIỄN THÔNG**

ĐỀ TÀI: TÌM HIỂU VÀ CẤU HÌNH WIFI

Cán bộ hướng dẫn : Nguyễn Quang Tú

Giảng viên hướng dẫn : TS. Đỗ Xuân Thu

Sinh viên : Nguyễn Thị Thanh Xuân

Mã sinh viên : 68DCDT20128

Lớp : 68DCDT22

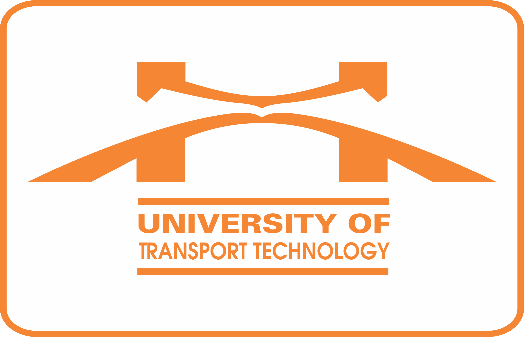
**HÀ NỘI - 2020**

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ GIAO THÔNG

VẬN TẢI

**-----🙞🙜🕮🙞🙜-----**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO THỰC TẬP TỐT NGHIỆP**

**Ngành: CNKT ĐIỂN TỬ - VIỄN THÔNG**

ĐỀ TÀI: TÌM HIỂU VÀ CẤU HÌNH WIFI

Cán bộ hướng dẫn : Nguyễn Quang Tú

Giảng viên hướng dẫn : TS. Đỗ Xuân Thu

Sinh viên : Nguyễn Thị Thanh Xuân

Mã sinh viên : 68DCDT20128

Lớp : 68DCDT21

**HÀ NỘI - 2020**

# **MỤC LỤC**

# **LỜI CẢM ƠN**

Sau quá trình thực tập tại Công ty TNHH hạ tầng viễn thông Miền Bắc em đã có rất nhiều kiến thức bổ ích. Nhờ sự giúp đỡ tận tình của các anh chị trong công ty đặc biệt là anh Nguyễn Quang Tú, người đã tận tình hướng dẫn em trong suốt quá trình thực tập giúp em hoàn thành bài báo cáo.

Em xin chân thành cảm ơn thầy Đỗ Xuân Thu giảng viên đã trực tiếp tận tình hướng dẫn em xuyên suốt quá trình làm báo cáo thực tập này. Cảm ơn thầy vì đã giúp chúng em có thêm cơ hội để biết thêm nhiều kiến thức mới và được vận dụng những kiến thức mà chúng em đã học.

Bên cạnh đó, em cũng xin cảm ơn ban giám hiệu nhà trường, các thầy cô trong Khoa Công nghệ Thông tin và các phòng ban nhà trường đã tạo điều kiện tốt nhất cho em cũng như các bạn khác trong suốt thời gian học tập và làm báo cáo.

Em rất mong quý công ty và các thầy cô cùng các bạn sinh viên có thế góp ý để em có thể hoàn thiện tốt hơn và làm đề tài thiện hơn trong quá trình thực tập này.

Em xin chân thành cảm ơn!

*Hà Nội, ngày.... tháng.... năm 2020.*

Sinh viên

Nguyễn Thị Thanh Xuân.

# **DANH MỤC KÝ HIỆU VÀ VIẾT TẮT**

|  |  |  |
| --- | --- | --- |
| **Kí hiệu** | **Tên tiếng Anh** | **Tên tiếng Việt** |
| TIN Telecom | Telecom Infrastructure North | [Công Ty TNHH Hạ Tầng Viễn Thông Miền Bắc](https://mywork.com.vn/tuyen-dung/nha-tuyen-dung/101416/cong-ty-tnhh-ha-tang-vien-thong-mien-bac-tin-(-doi-tac-fpt-telecom).html) |
| IEEE | Institute of Electrical and Electronics Engineers | Hội kỹ sư điện và điện tử |
| FPT | Financing Promoting Technology | Công ty Đầu tư và Phát triển Công nghệ (Công ty cổ phần FPT) |
| LAN | Local Network Area | Mạng cục bộ |
| WAN | Wide Area Network | Mạng diện rộng |
| SSID | Service Set Identifier | Mạng cục bộ không dây |
| ADSL | [Asymmetric Digital Subscriber Line](https://sk.wikipedia.org/wiki/Asymmetric_Digital_Subscriber_Line) | Công nghệ cung cấp tốc độ truyền cao cho video và giọng nói |
| FHSS | Frequency Hopping Spread Spectrum | Phổ trải rộng nhảy tần số |
| TDMA | Time Division Multiple Access | Phương thức đa truy cập phân chia theo thời gian |
| TDM | Time Division Multiplexer | Bộ ghép kênh phân chia thời gian |
| WDM | Wave Division Multiplexing | Phương thức ghép kênh quang theo bước sóng. |
| WAP | Wireless Access Point | Điểm truy cập Wireless |
| CDMA | Code Division Multiple Access | Đa truy nhập (đa người dùng) phân chia theo mã. |
| AOM | Acute Otitis Media | Phương thức truy nhập |
| DT | Data Transmitsion | Dữ liệu vào |
| DR | Data Receiver | Dữ liệu ra |

**LỜI NÓI ĐẦU**

Chúng ta đang sống trong một thời đại mới, thời đại phát triển của công nghệ thông tin, đặc biệt là công nghệ máy tính và mạng máy tính với sự bùng nổ của hàng ngàn cuộc cách mạng lớn nhỏ. Sự ra đời của mạng máy tính và những dịch vụ của nó đã mang lại cho con người rất nhiều những lợi ích to lớn, góp phần thúc đẩy nền kinh tế phát triển, đơn giản những thủ tục lưu trữ, xử lý, truyền thống tin phức tạp và liên lạc và kết nối giữa những vị trí, khoảng cách lớn một cách nhanh chóng, hiệu quả. Vì mạng máy tính đã trở thành yếu tố không thể thiếu đối với sự phát triển của nền kinh tế, chính trị cũng như văn hóa của các quốc gia. Mạng máy tính được hình thành từ nhu cầu muốn chia sẻ tài nguyên và dùng chung nguồn dữ liệu. Nhà quản lý có thể sử dụng các chương trình tiện ích để giao tiếp truyền thông nhanh chóng và hiệu quả với rất nhiều người cũng như để tổ chức sắp xếp cho toàn công ty dễ dàng. Nếu không có hệ thống mạng, dữ liệu phải được in ra giấy thì người khác mới có thể hiệu chỉnh và sử dụng được hoặc có thể sao chép lên đĩa mềm do tốn nhiều thời gian và công sức.

Cũng vì vậy, nếu không có mạng máy tính, hoặc mạng máy tính không thể hoạt động như ý muốn thì hậu quả sẽ rất nghiêm trọng. Và vấn đề an toàn cho mạng máy tính cũng phải đặt lên hàng đầu khi thiết kế, lắp đặt và đưa vào sử dụng một hệ thống mạng máy tính dù đơn giản nhất.

Bên cạnh đó, thông tin giữ một vai trò hết sức quan trọng bởi vì nếu như thiếu thông tin, con người sẽ trở nên lạc hậu dẫn tới những hậu quả nghiêm trọng, nền kinh tế chậm phát triển. Vì vậy, việc lưu giữ, trao đổi và quản lý tốt nguồn tài nguyên thông tin để sử dụng đúng mục đích, không bị thất thoát đã là mục tiêu hướng tới của không chỉ một nghành, một quốc gia mà của toàn thế giới.

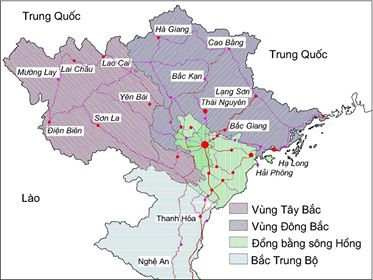
Vì vậy em muốn tìm hiểu về đề tài mạng máy tính và tường lửa. Do vốn kiến thức của bản thân còn chưa rộng, thời gian, điều kiện tiếp xúc thực tiễn và nghiên cứu còn hạn chế nên em chưa tìm hiểu và trình bày thật sự tốt và kỹ lưỡng về vấn đề nghiên cứu. Trên đây là những kiến thức em đã tìm hiểu và nắm được trong quá trình thực tập, nghiên cứu và qua sự hướng dẫn, chỉ bảo tận tình của thầy giáo Đỗ Xuân Thu. Em rất cảm ơn và mong nhận được sự giúp đỡ, chỉ bảo hơn nữa của thầy và của các thầy, các cô để có thể trang bị thêm cho mình những kiến thức cần thiết về đề tài em đã nêu trên. Những kiến thức đó và những kiến thức đã được trang bị trong quá trình học tập, nghiêm cứu tại trường cũng là cái gốc để từ đó em có cơ sở nghiên cứu, phát huy tiếp về đề tài này.

Em xin chân thành cảm ơn!

**PHẦN A: GIỚI THIỆU VỀ CÔNG TY TNHH HẠ TẦNG VIỄN THÔNG MIỀN BẮC (TIN)**

* 1. **Giới thiệu chung về công ty**

Công ty TNHH Hạ tầng Viễn thông Miền Bắc (TIN) thành lập ngày 01/04/2010, là đơn vị đối tác độc quyền của FPT Telecom tại khu vực Miền Bắc và Miền Trung. Trải qua hơn 6 năm hoạt động trong lĩnh vực triển khai- bảo trì dịch vụ viễn thông, TIN nhanh chóng gây dựng cho mình một đội ngũ cán bộ nhân viên đông đảo với trên 2.500 nhân sự có chuyên môn và bề dày kinh nghiệm, trải dài trên 29 tỉnh thành. Với Slogan "Chất lượng tạo niềm tin”, TIN đã khẳng định được vị thế vững chắc của mình trong lĩnh vực triển khai- bảo trì dịch vụ viễn thông trên toàn quốc và luôn là đối tác độc quyền- đáng tin cậy của FPT Telecom.

* 1. **Phạm vi hoạt động của công ty**

Hình A.1. Phạm vi hoạt động.

Trung tâm kỹ thuật TIN bố trí rộng khắp 28 tỉnh thành Miền Bắc và Miền Trung.  Riêng địa bàn thủ đô Hà Nội TIN có 4 trung tâm lớn hoạt động mạnh, đảm bảo phục vụ triển khai, bảo trì nhanh chóng, thuận lợi, tiết kiệm tối đa thời gian, giảm thiểu lãng phí không cần thiết cho tất cả các đối tượng Quý khách hàng.

+ Trung tâm 1: Số 79, lô TT 2, X5, phường Mỹ Đình 2, quận Nam Từ Liêm, Hà Nội.

+ Trung tâm 2: Số 47, Lô 5,  khu Đền Lừ 2, quận Hoàng  Mai, Hà Nội.

+ Trung tâm 3: Số LK 21, khu liền kề 6A, làng Việt Kiều Châu Âu, Mỗ Lao, Hà Đông, Hà Nội.

+ Trung tâm hỗ trợ doanh nghiệp: Số 51, ngõ 155 Nguyễn Khang, quận Cầu Giấy, Hà Nội.

**Địa bàn hoạt động:**

Bảng A.2. Địa bàn hoạt động của công ty

|  |  |
| --- | --- |
| **Đơn vị** | **Địa Bàn** |
| HN1 | Ba Đình, Hồ Tây |
| HN2 | Hoàn Kiếm, Hai Bà Trưng |
| HN3 | Đống Đa |
| HN4 | Hoàng Mai |
| HN5 | Thanh Xuân |
| HN6 | Cầu Giấy |
| HN7 | Long Biên, Gia Lâm |
| HN8 | Nam Từ Liêm, Hoài Đức, Quốc Oai |
| HN9 | Đông Anh, Mê Linh, Sóc Sơn |
| HN10 | Hà Đông, Chương Mỹ, |
| HN11 | Thanh Trì, Thường Tín, Phú Xuyên |
| HN12 | Thanh Oai, Ứng Hoài |
| HN13 | Bắc Từ Liêm, Đan Phượng, Phúc Thọ |
| HN14 | Sơn Tây, Thạch Thất, Ba Vì |

**1.3.Lĩnh vực hoạt động của công ty**

Công ty TNHH hạ tầng viễn thông Miền Bắc - đối tác độc quyền duy nhất hoạt động chuyên nghiệp lĩnh vực kỹ thuật viễn thông của FPT Telecom khu vực Miền Bắc và Miền Trung:

+ Triển khai, bảo trì, chuyển địa điểm mạng lưới internet tốc độ cao.

+ Lắp đặt dịch vụ truyền hình PayTV với nhiều kênh truyền hình HD, kho phim HD, các tính năng giải trí khác hấp dẫn, chất lượng hình ảnh và âm thanh tuyệt hảo.

+ Nâng cấp chuyển đổi công nghệ cáp quang mới, hiện đại ( FTTH new) từ hạ tầng công nghệ cáp đồng ( ADSL) đã lạc hậu của FPT.

Niềm tin khách hàng dành cho, hiệu suất cao trong quá trình làm việc đã xây dựng tên tuổi TIN hôm nay.

* 1. **Chức năng, nhiệm vụ**
     1. **Nhân viên kỹ thuật**
* Lắp đặt đường truyền Internet cho khách hàng
* Kiểm tra, sửa lỗi tín hiệu đường dây Internet bị lỗi cho khách hàng
* Cài đặt các dịch vụ khác (One TV, truyền hình cáp…) do FPT Telecom cung cấp cho khách hàng
* Hỗ trợ kĩ thuật trực tiếp cho khách hàng theo yêu cầu
  + 1. **Kỹ thuật viên**
* Hỗ trợ trực tiếp tại nhà khách hàng
* Bảo hành, bảo trì thiết bị cho khách hàng
* Phối hợp xử lý thông tin, hỗ trợ kĩ thuật
  + 1. **Điều hành kỹ thuật**
* Quản lý, điều hành công việc của nhân viên kỹ thuật, kỹ thuật viên
* Đôn đốc, giám sát các tổ, nhóm thi công, điều phối công việc
* Làm, gửi báo cáo định kỳ, đột xuất. Tổng hợp phân tích số liệu
* Phối hợp xử lý thông tin, hỗ trợ kỹ thuật với các bộ phận liên quan
* Xử lý các công việc phát sinh
  + 1. **Đội ngũ nhân sự**

Tại sao dịch vụ dành cho khách hàng được thực hiện nhanh chóng, hoàn hảo. Đơn giản TIN có sự phối hợp nhuần nhuyễn giữa lãnh đạo với các phòng ban, giữa các phòng ban với nhau, sự kết hợp nhịp nhàng giữa đội ngũ nhân viên văn phòng với đội ngũ kỹ thuật viên. Họ là những con người ưu tú, nhiệt huyết với công việc.

Lãnh đạo, quản lý TIN được đào tạo bài bản trong nước và nước ngoài chuyên môn ngành công nghệ thông tin, kinh tế, kỹ thuật viễn thông, là những người vạch kế hoạch, đưa ra giải pháp, sẵn sàng đi tiên phong trong thời đại kinh tế Việt Nam cạnh tranh quyết liệt.

Nhân viên văn phòng, nhân viên kỹ thuật TIN năng động, nghiệp vụ cao , thân thiện, phẩm chất đạo đức tốt, dày dặn kinh nghiệm triển khai, bảo trì, kiểm tra lắp đặt, nâng cấp chuyển đổi hạ tầng.

Khu vực triển khai thi công địa hình, địa vật phức tạp TIN đều có giải pháp, phương án hợp lý nên kế hoạch thi công. Hầu hết đội ngũ nhân viên TIN được chon lọc kỹ lưỡng từ các trường đại học hàng đầu về ngành Công Nghệ Thông Tin.

An toàn lao động, tác phong nhân viên, chất lượng kỹ thuật dịch vụ được TIN đưa lên hàng đầu. Việc kiểm tra, kiểm soát chặt chẽ thực tế là nghĩa vụ thường xuyên của đội ngũ thanh tra TIN.

Các khóa đào tạo kỹ năng mềm, nghiệp vụ chuyên môn cho nhân viên toàn TIN được phòng nhân sự tổ chức định kỳ, hiệu quả, không ngừng nâng cao chất lượng đội ngũ nhân sự.

* 1. **Tri ân khách hàng**

Mục tiêu chiến lược tương lai, TIN không ngừng hoàn thiện con người, chất lượng kỹ thuật, chất lượng vật tư thiết bị và luôn lắng nghe tiếp thu ý kiến đóng góp quý báu từ khách hàng và đồng nghiệp.

Mong muốn chúng tôi ngày càng hoàn thiện, phát triển mạnh hơn trong hoạt động triển khai, bảo trì trạn BTS, chuyển đổi hạ tầng kỹ thuật viễn thông của TIN.

* 1. **Tổng kết**

Sau khi tìm hiểu thêm về công ty thì em thấy rằng đây là một môi trường rất năng động, trẻ trung, rất phù hợp để em có thể học hỏi kinh nghiệm của các anh chị đi trước cũng như là trau dồi thêm kiến thức để có thêm sự tự tin khi bước ra môi trường thực tế.

Đây là những hành động cụ thể theo 5 định hướng chính của công ty mà em đang tìm hiểu:

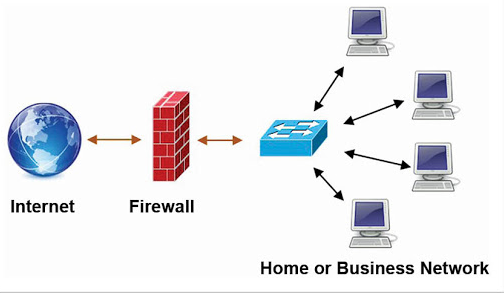
* Nâng cao giá trị gia tăng cho sản phẩm dịch vụ (Move up IT Value Chain).
* Chủ động tìm kiếm và cung cấp giải pháp công nghệ tầm quốc gia.
* Nghiên cứu phát triển và ứng dụng thương mại hóa công nghệ.
* Phát triển nguồn nhân lực công nghệ.
* Hiện đại hóa quản trị FPT.

**PHẦN B: TÌM HIỀU VỂ FIREWALL**

**CHƯƠNG I: TỔNG QUAN VỀ FIREWALL**

**1.1 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 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. 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.



Hình 1.1: Mô hình chức năng của tường lửa

Bức tường lửa (Firewall) hiểu một cách chung nhất, là cơ cấu để bảo vệ một mạng máy tính chống lại sự truy nhập bất hợp pháp từ các (mạng) máy tính khác. Firewall bao gồm các cơ cấu nhằm:

* Ngăn chặn truy nhập bất hợp pháp.
* Cho phép truy nhập sau khi đó kiểm tra tính xác thực của thực thể yêu cầu truy nhập.

Trên thực tế, Firewall được thực hiện rất khác nhau: bằng phần mềm hoặc phần cứng chuyên dùng, sử dụng một máy tính hoặc một mạng các máy tính... Theo William Cheswick và Steven Beilovin thì bức tường lửa có thể được xác định như là một tập hợp các cấu kiện đặt giữa hai mạng.

* **Nhìn chung bức tường lửa có những thuộc tính sau:**
* Thông tin giao lưu được hai chiều.
* Chi những thông tin thảo mãn nhu cầu bảo vệ cục bộ mới được đi qua.
* Bản thân bước tường lửa không đòi hỏi quá trình thâm nhập.
* **Firewall làm được những gì?**

Nhìn chung, Firewall có thể bảo vệ hệ thống máy tính chống lại những kẻ đột nhập qua khả năng ngăn chặn những phiên làm việc từ xa (remote login).

Ngăn chặn thông tin từ bên ngoài (Internet) vào trong mạng được bảo vệ, trong khi cho phép người sử dụng hợp pháp được truy nhập tự do mạng bên ngoài.

Firewall còn là một điểm quan trọng trong chính sách kiểm soát truy nhập. Nó là “cửa khẩu” duy nhất nối mạng được bảo vệ với bên ngoài, do đó có thể ghi nhận mọi cuộc trao đổi thông tin, điểm xuất phát và đích, thời gian,... Firewall có thể phục vụ như một công cụ theo dõi các cuộc tấn công với ý đồ xấu từ bên ngoài nhằm dự báo khả năng bị tấn công trước khi cuộc tấn công xảy ra.



Hình 1.2. Hình ảnh lợi ích của Firewall

* **Firewall không làm được những gì?**

Firewall không đủ thông minh như con người 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 nhưng 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 đường 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 chương trình được chuyển theo thư điện tử, vượt qua Firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được 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 được áp dụng rộng rãi.

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.

**1.2 Chức năng:**

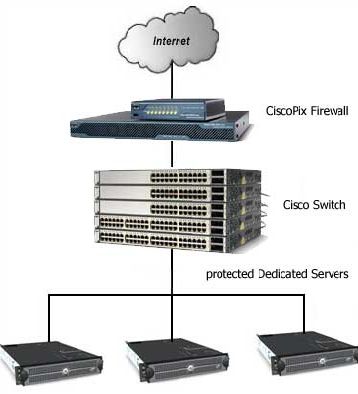
Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:

* Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).
* Cho phép hoặc cấm những dịch vụ  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.

**1.3.Phân loại:**

**1.3.1 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 tưởng lửa).

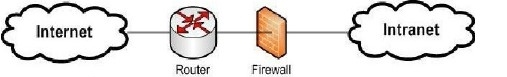


Hình 1.3: Mô hình các thiết bị phần cứng của Firewall

**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 nột dung của gói tin.

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



Hình 1.4: Hình ảnh Firewall cứng

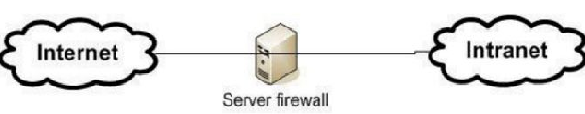
**1.3.2 Firewall mềm:**

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) Firewal mềm có thể kiểm tra được nội dung của gói tin (thông qua các từ khóa).

**Ví dụ về Firewall mềm**: Zone Alarm, Norton Firewall…



Hình 1.5. Hình ảnh Firewall mềm

**1.3.4.Các sản phẩm firewall**

* **Software firewalls**

– Software firewalls – firewall mềm – là những firewall được cài đặt trên một hệ điều hành. Firewall mềm bao gồm các sản phẩm như SunScreen firewall, IPF, Microsoft ISA server, Check Point NG, Linux’s IPTables …Firewall mềm thường đảm nhận nhiều vai trò hơn firewall cứng, nó có thể đóng vai trò như một DNS server hay một DHCP server.

– Một nhược điểm của firewall mềm là nó được cài đặt trên một hệ điều hành và do đó khả năng có lỗ hổng trên hệ điều hành này là có thể xẩy ra. Khi lỗ hổng được phát hiện và được cập nhật bản vá lỗi, rất có thể sau khi cập nhật bản vá lỗi cho hệ điều hành thì firewall không hoạt động bình thường như trước, do đó cần tiến hành cập nhật bản vá cho firewall từ nhà cung cấp sản phẩm firewall.

– Một ưu điểm nổi trội của firewall mềm là việc thay đổi và nâng cấp thiết bị phần cứng là tương đối dễ dàng và nhanh chóng.

– Do hệ điều hành mà firewall mềm chạy trên nó không được thiết kế tối ưu cho firewall nên firewall mềm có hiệu suất thấp hơn firewall cứng.

* **Appliance firewalls**

– Appliance firewalls – firewall cứng – là những firewall được tích hợp sẵn trên các phần cứng chuyên dụng, thiết kế dành riêng cho firewall. Các sản phẩm firewall cứng đáng chú ý như Cisco PIX, NetScreen firewall, SonicWall Appliaces, WatchGuard Fireboxes, Nokia firewall…

– Trong nhiều trường hợp firewall cứng cung cấp hiệu suất tốt hơn so firewall mềm vì hệ điều hành của firewall cứng được thiết kế để tối ưu cho firewall.

– Lợi ích điển hình khi sử dụng firewall cứng là hiệu suất tổng thể tốt hơn firewall mềm, tính bảo mật được nâng cao, tổng chi phí thấp hơn so với firewall mềm.

– Firewall cứng không được linh hoạt như firewall mềm ( không thể thêm chức năng, thêm các quy tắc như trên firewall mềm)

– Hạn chế của firewall cứng là khả năng tích hợp thêm các chức năng bổ sung khó khăn hơn firewall mềm, chẳng hạn như chức năng kiểm soát thư rác đối với firewall mềm chỉ cần cài đặt chức năng này như một ứng dụng còn đối với firewall cứng phải có thiết bị phần cứng hỗ trợ cho chức năng này.

* **Integrated firewalls**

– Integrated firewalls – firewall tích hợp – ngoài chức năng cơ bản của firewall thì nó còn đảm nhận các chức năng khác như VPN, phát hiện phòng chống xâm nhập, lọc thư rác, chống virus. Lợi ích của việc dùng firewall tích hợp là đơn giản hóa thiết kế mạng bằng cách giảm lượng thiết bị mạng cũng như giảm chi phí quản lý, giảm gánh nặng cho các chuyên viên quản trị, ngoài ra nó còn tiết kiệm chi phí hơn so với việc dùng nhiều thiết bị cho nhiều mục đích khác nhau.

– Tuy nhiên việc tích hợp nhiều chức năng trên cùng một thiết bị dẫn đến khó khăn trong khắc phục sự cố vì tính phức tạp của hệ thống khi tích hợp.

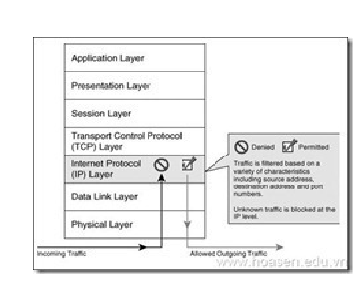
**1.4. Các công nghệ firewall**

Dựa vào công nghệ sử dụng trong firewall người ta chia firewall thành các loại như sau:

* Personal firewalls
* Packet filters
* Network Address Translations (NAT) firewalls
* Circuit-level firewalls
* Proxy firewalls
* Stateful firewalls
* Transparent firewall
* Virtual firewalls

– Personal firewalls: Được thiết kế để bảo vệ một host duy nhất, thường được tích hợp sẵn trong các laptop, desktop…

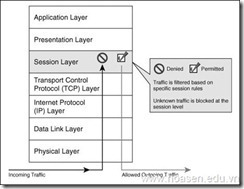
– Packet filters: Là thiết bị được thiết kế để lọc gói tin dựa trên những đặc điểm đơn giản của gói tin. Packet filters tiêu biểu cho dạng statless vì nó không giữ bảng trạng thái các kết nối và không kiểm tra trạng thái các kết nối.



* **Packet filtering firewall**

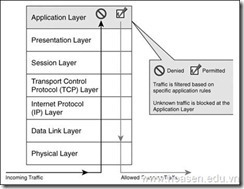
– Network Address Translations (NAT) firewalls: Thực hiện chức năng chuyển đổi địa chỉ IP public thành địa IP private và ngược lại, nó cung cấp cơ chế che dấu IP các host bên trong.

– Circuit-level firewalls: Hoạt động tại lớp session của mô hình OSI, nó giám sát các gói tin “handsahking” đi qua firewall, gói tin được chỉnh sửa sao cho nó xuất phát từ circuit-level firewall, điều này giúp che dấu thông tin của mạng được bảo vệ.

[](https://nguyentanvy.files.wordpress.com/2011/11/clip_image007.jpg)

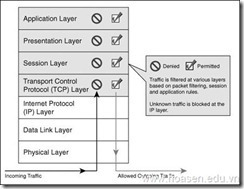
* **Circuit-Level Firewall**

– Proxy firewalls: Hoạt động tại lớp ứng dụng của mô hình OSI, nó đóng vai trò như người trung gian giữa hai thiết bị đầu cuối. Khi người dùng truy cập dịch vụ ngoài internet, proxy đảm nhận việc yêu cầu thay cho client và nhận trả lời từ server trên internet và trả lời lại cho người dùng bên trong.

[](https://nguyentanvy.files.wordpress.com/2011/11/clip_image009.jpg)

* **Proxy firewall**

– Stateful firewalls: Được kết hợp với các firewall khác như NAT firewall, circuit-level firewall, proxy firewall thành một hệ thống firewall, nó không những kiểm tra các đặc điểm của gói tin mà lưu giữ và kiểm tra trạng thái của các gói tin đi qua firewall, một ví dụ cho statefull firewall là sản phẩm PIX firewall của Cisco.

[](https://nguyentanvy.files.wordpress.com/2011/11/clip_image011.jpg)

* **Statefull firewall**

– Transparent firewall: Hoạt động ở layer 2 của mô hình OSI, nó hỗ trợ khả năng lọc các gói tin IP (bao gồm IP, TCP, UDP và ICMP). Transparent firewall thực chất chỉ là tính năng layer 2 brigde kết hợp với tính năng filter trên nền IP bằng cách sử dụng tính năng Context Based Access Control. Vì nó hoạt động ở layer 2 nên ta không cần cấu hình IP cũng như thay đổi IP của các thiết bị được nó bảo vệ.

– Virtual firewalls: Bao gồm nhiều logical firewall hoạt động trên một thiết bị thật. Một trong những ứng dụng của nó hiện nay là dùng trong việc quản lý các máy ảo trong vmware hay hyper-v.

**1.5. Firewall mã nguồn mở và firewall mã nguồn đóng**

Có nhiều loại firewall trên thị trường hiện nay, một loại là mã nguồn mở như Linux IPTables, OpenDSD pf, Solaris IPF firewalls, và một loại khác là mã nguồn đóng như Cisco PIX, ASA firewall, Juniper ScreenOS, Check Point’s firewall. Sự khác biệt đáng chú ý nhất đối với hai loại firewall này là khả năng thương mại hóa của các firewall.

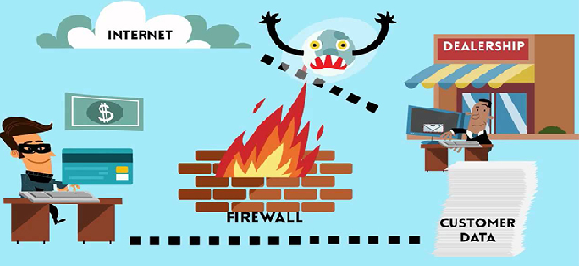
Hầu hết các firewall thương mại đều được tích hợp các tính năng thêm như VPN, phát hiện xâm nhập và khả năng kiểm tra sâu bên trong gói tin. Trong khi đó, các firewall mã nguồn mở chỉ tập trung vào việc lọc các gói tin mà không tích hợp thêm các chứng năng khác và nhường chổ các chức năng này cho các phần mềm khác.

**1.6. Nguyên lí 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, SMNP, 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

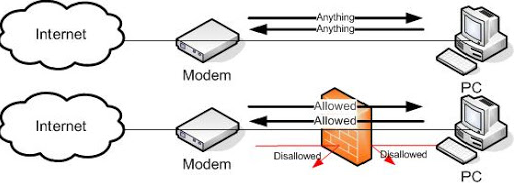
Nếu packet thỏa các luật lệ đã được thiết lập trước của Firewall thì packet đó được chuyển qua, nếu không thỏa thì sẽ bị loại bỏ. Việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định được phép mới vào được hệ thống mạng cục bộ.



Hình 1.8 Cách thức hoạt động của Firewall

Cũng nên lưu ý là do việc kiểm tra dựa trên header của các packet nên bộ lọc không kiểm soát được nội dụng 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.

**1.7.Ứng dụng của Firewall:**

****

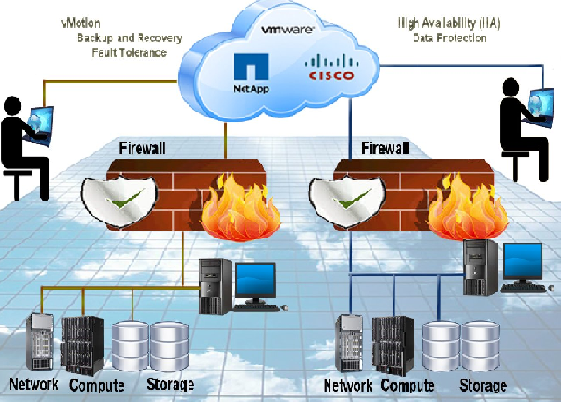
Hình 1.6. Chức năng của Firewall

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 cuả 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 cuả 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.

**1.7.1.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 mât, tính toàn vẹn và tính kịp thời.
* Tài nguyên hệ thống.
* Danh tiếng của công ty sở hữu các thông tin cần bảo vệ.



Hình 1.7 Hình ảnh vai trò của Firewall

**1.7.2.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 như chương trình dò 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 hoá 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.

**1.8. Kết luận**

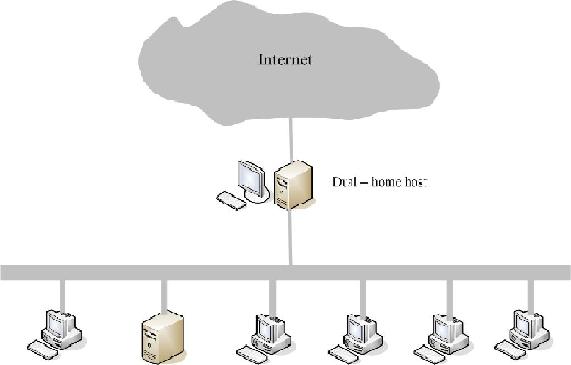
**CHƯƠNG II: NHỮNG THIẾT KẾ CƠ BẢN CỦA FIREWALL**

Dưới đây sẽ đưa ra một số kiến trúc Firewall cơ bản, các kiến trúc khác có thể mở rộng từ kiến trúc này tùy theo cấu trúc kết nối của mạng.

**2.1. 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 dual - homed host rất đơn giản, máy dual - homed host ở giữa, một bên được nối với internet và bên còn lại nới với mạng nội bộ (mạng cần được bảo vệ).

Dual – homed Host là hình thức xuất hiện đầu tiên trong cuộc đấu để bảo vệ mạng nội bộ. Dual – homed Host là một máy tính có hai giao tiếp mạng: một nối với mạng cục bộ và nối với mạng ngoài (Internet).



Hình 2.1: Kiến trúc Dual – homed Host

Hệ điều hành của Dual – homed Host được sửa đổi để chức năng chuyển các gói tin (Packet forwarding) giữa hai giao tiếp mạng này không hoạt động. Để làm việc được với một máy trên Internet, người dùng ở mạng cục bộ trước hết phải login vào Dual – homed Host, và từ đó bắt đầu phiên làm việc.

**Gồm có các đặc điểm sau:**

* Phải disable chức năng routing của dual-homed host để cấm hòan toàn lưu thông IP từ ngòai vào.
* Các hệ thống bên trong và bên ngoài dual-homed host chỉ có thể liên lạc với dual-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 vào dual-homed host.
* **Ưu điểm và nhược điểm của Dual – homed Host:**
* **Ưu điểm của Dual – homed Host:**
* Cài đặt dễ dàng, không yêu cầu phần cứng hoặc phần mềm đặc biệt.
* Dual – homed Host chỉ yêu cầu cấm khả năng chuyển các gói tin, do vậy thông thường trên các hệ Unix, chỉ cần cấu hình và dịch lại nhaamn (Kernel) của hệ điều hành là đủ.
* **Nhược điểm của Dual – homed Host:**
* Không đáp ứng được những yêu cầu bảo mật ngày càng phức tạp, cũng như những hệ phần mềm mới được tung ra thị trường.
* Không có khả năng chống đỡ những cuộc tấn công nhằm vào chính bản thân nó, và khi Dual – homed Host đó bị đột nhập, nó sẽ trở thành đầu cầu lý tưởng để tấn công vào mạng nội bộ.
* **Đánh giá về kiến trúc Dual – homed Host:**

Để cung cấp dịch vụ cho những người sử dụng internal network có một số giải pháp như sau:

* Kết hợp với các Proxy Server cung cấp những Proxy Service.
* Cung cấp account cho user trên mạng máy dual-homed host này và khi mà người sử dụng muốn sử dụng dịch vụ từ internet hay dịch vụ từ external network thì họ phải logginh thì họ phải logging in vào máy này.

Nếu dùng phương pháp cấp account cho user trên máy dual-homed hót thì user không thích sử dụng dịch vụ phiền phức như vậy, vì mỗi lần họ muốn sử dụng dịch vụ thì phải logging in vào máy khác, khác với máy của họ đây là vấn đề rất là không trong suốt với người sử dụng.

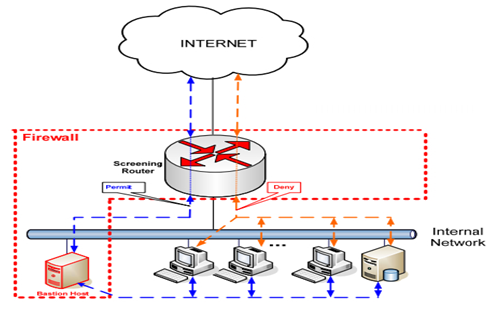
Nếu dùng Prosy Server: khó có thể cung cấp được nhiều dịch vụ cho người sử dụng vì phần mềm Proxy Server và Proxy Client không phải laoij dịch vụ nào cũng có sẵn. Hoặc khi số dịch vụ cung cấp nhiều thì khả năng đáp ứng của hệ thống có thể giảm xuống vì tất cả các Proxy Server đều đặt trên cùng một máy.

Một khuyết điểm cơ bản của hai mô hình trên nữa là: khi mà máy dual – homed host nói chung cũng như các Proxy Server bị đột nhập vào. Người tấn công độ nhập vào được qua nó thì lưu thông bên trong Internal network bị attacker này thấy hết điều này thì hết sức nguy hiểm. Trong các hệ thống mạng dùng Ethernet hoặc Token Ring thì dữ liệu lưu thông trong hệ thống có thể bị bất kỳ máy nào nối vào mạng đánh cắp dữ liệu cho nên kiens trúc trên chỉ thích hợp với một số mạng nhỏ.

**2.2. 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).



Hình 2.2: Kiến trúc Screened Host

Kiến trúc này kết hợp 2 kỹ thuật đó là Packet Filtering và Proxy Services.

Packet Filterning: Lọc một số loại dịch vụ mà hệ thống muốn cung cấp sử dụng Proxy Server, bắt người sử dụng nếu muốn dùng dịch vụ thì phải kết nối đến Proxy Server mà không được bỏ qua Proxy Server để nối trực tiếp với mạng bên trong/bên ngoài (internal/external network), đồng thời có thể cho phép Bastion Host mở một số kết nối với internal/external host.

Proxy Service: Bastion Host sẽ chứa các Proxy Server để phục vụ một số dịch vụ hệ thống cung cấp cho người sử dụng qua Proxy Server.

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.

* **Đánh giá một số ưu, khuyết điểm chính của kiến trúc Screened Host**

Kiến trúc screened host hay hơn kiến trúc dual-homed host ở một số điểm cụ thể:

* Dual – homed Host: Khó có thể bảo vệ tốt vì máy này cùng lúc cung cấp nhiều dịch vụ, vi phạm qui tắc căn bản là mỗi phần tử hay thành phần nên giữ ít chức năng nếu có thể được (mỗi phần tử nên giữ ít chức năng càng tốt), cũng như tốc độ đáp ứng khó có thể vì cùng lúc đảm bảo nhận nhiều chức năng.
* Screened Host: Đã tách chức năng lọc các gói IP và các Proxy Server ở hai máy riêng biệt. Packet Filtering chỉ giữ chức năng lọc gói nên có thể kiểm soát, cũng như khó xảy ra lỗi (tuân thủ qui tắc ít chức năng). Proxy Servers được đặt ở máy khác nên khả năng phục vụ (tốc độ đáp ứng) cũng cao.

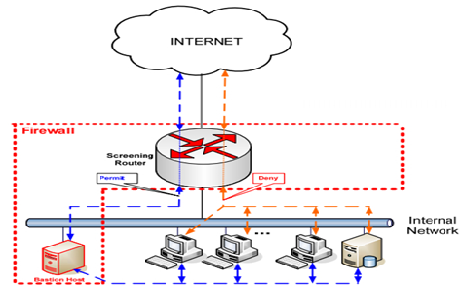
Cũng tương tự như kiến trúc Dual- Homed Host khi mà Packet Filtering system cũng như Bastion Host chứa các Proxy Server bị đột nhập vào (người tấn công đột nhập được qua ccs hàng rào này) thì lưu thông của internal network bị người tấn công thấy.

Từ khuyết điểm chính của 2 kiến trúc trên ta có kiến trúc thứ 3 sau đây khắc phục được phần nào khuyết điểm trên.

**2.3. Kiến trúc Screened Subnet Host**

Thêm một 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.



Hình 2.3: Kiến trúc Screened Subnet Host

Với kiến trúc này, hệ thống này bao gồm hai Packet-Filtering Router và một Bastion Host. Kiến trúc này có độan toàn cao nhất vì nó cung cấp cả mức bảo mật: Network và Application trong khi định nghĩa một mạng perimeter network. Mạng trung gian (DMZ) đóng vai trò như một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một DMZ được cấu hình sao cho các hệ thống trên mạng DMZ, và sự truyền trực tiếp qu mạng DMZ là không thể được.

Với những thông tin đến, Router ngoài (Exterior Router) chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP), và điều khiển truy nhập tới DMZ. Nó chỉ cho phép hệ thống bên ngoài truy nhập Bastion Host, Router trong (Interior Router) cung cấp sự bảo vệ thứ hai bằng điều khiển DMZ truy nhập mạng nội bộ chỉ với những truyền thông bắt đầu từ Bastion Host.

Với những thông tin đi, Router trong điều khiển mạng nội bộ truy nhập tới DMZ. Nó chỉ cho phép các hệ thống bên trong truy nhập Bastion. Quy luật Filtering trên Router ngoài yêu cầu sử dụng dịch vụ Proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ Bastion Host.

* **Ưu điểm:**
* Kẻ tấn công cần phá vỡ ba tầng bảo vệ: Router ngoài, Bastion Host và Router trong.
* Bởi vì Router ngoài chỉ quảng bá DMZ Network tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là được biết đến bởi Internet qua routing table và DNS information exchange (Domain Name Server).
* Bởi vì Router trong chỉ quảng cáo DMZ Network tới mạng nội bboj, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều này đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ Proxy.
* **Đánh giá về kiến trúc Screened Subnet host:**

Đối với những hệ thống yêu cầu cung cấp dịch vụ nhanh, an toàn cho nhiều người sử dụng đồng thời cũng như khả năng theo dõi lưu thông của mỗi người sử dụng trong hệ thống và dữ liệu trao đổi giữa các người dùng trong hệ thống cần được bảo vệ thì kiến trúc cơ bản trên phù hợp.

Để tăng độ an toàn trong internal network, kiến trúc screen subnet ở trên sử dụng thêm mọt mạng DMZ (DMZ hay perimeter network) để che phần nào lưu thông bên trong internal network. Tách biệt internal network với Internet.

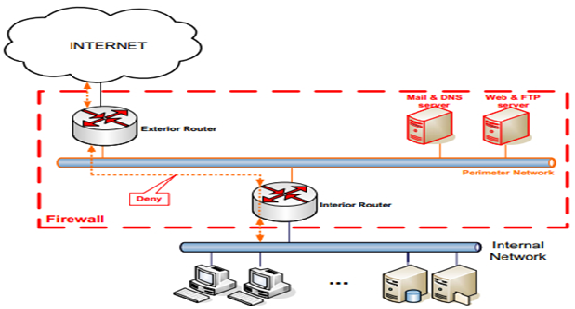
Sử dụng 2 Screening Router: Extenrion Router và Interrior Router.

Áp dụng qui tắc dư thừa có thể bổ sung thêm nhiều mạng trung gian (DMZ hay perimeter network) càng tăng khi khả năng bảo vệ càng cao. Ngoài ra, còn có những kiến trúc biến thể khác như: sử dụng nhiều Bastion Host, ghép chung Bastion Host và Router ngoài.

**2.4. 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).

Do các yêu cầu về tốc độ đáp ứng (performance) và dư thừa (redundancy), cũng như tách biệt các Servers khác nhau.



Hình 2.4. Kiến trúc sử nhiều Bastion Host

Sử dụng 1 Bastion Host cung cấp những dịch vụ cho người sử dụng bên trong (intrenal usre), như dịch vụ SNMP Server, Proxy Servers,...

Sử dụng 1 Bastion Host khác cung cấp dịch vụ cho Internet hoặc những người sử dụng bên ngoài (external user) sẽ sử dụng bên trong (local users) không truy xuất đến.

Với cách này thì tốc độ đáp ứng cho những người sử dụng bên trong (local user) một phần nào đó không bị ảnh hưởng (bị làm chậm đi) bởi hoạt động của những người sử dụng bên ngoài (extemal users).

Cũng có thể sử dụng nhiều Bastion Host mà cung cấp cho 1 dịch vụ nào đó để tăng tốc độ đáp ứng (performance), nhưng việc này cũng khó cân bằng tải giữa các Server trừ khi đoán trước được mức độ sử dụng.

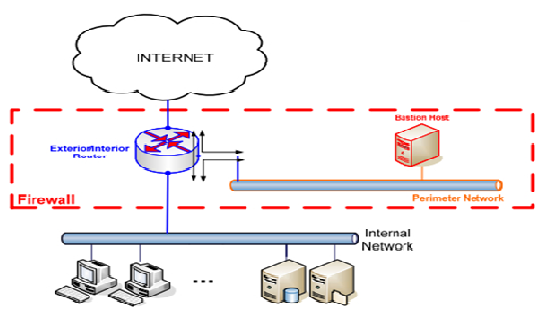
Việc sử dụng kỹ thuật dư thừa để đảm bảo tính sẵn sàng cao của hệ thống, để khi mà một Bastion Host hổng thì có cái khác thay thế. Nhưng chỉ có một số loại dịch vụ trợ giúp dạng này: DNS Server, SMTP Server.. có thể dùng nhiều Bastion Host làm DSN Server, SMTP Server. Khi một Bastion Host hỏng hoặc quá tải, những yêu cầu về DNS Server và SNMP sẽ được dùng qua Bastion Host khác như là một fallback system.

Sử dụng nhiều Bastion Host trong trường hợp muốn cung cáp dịch vụ cho nhiều mạng khác nhau, va loại dữ liệu cung cấp cho mỗi mạng cũng khác nhau.

Sử dụng iều Bastion Host cho các Server cho các Server khác nhau để khi mà một Server nào đó bị đột nhập vào hay bị hỏng thì Server khác vẫn hoạt động tốt. Ví dụ: Tách HTTP Server và FTP Server trên máy riêng biệt.

**2.5. 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.



Hình 2.5: Kiến trúc ghép chung Router trong và Router ngoài.

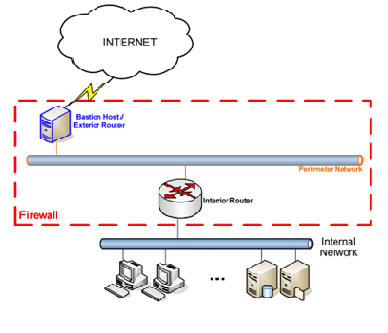
Do ghép chung router trong và router ngoài nên kiến trúc này làm giảm đi lớp bảo vệ mạng bên trong, có thể nói kiến trúc ghép chung router trong và router ngoài nằm ở giữa kiến trúc Screened host và Screened Subnet host.

Sử dụng kiến trúc này thì cần tăng tốc độ của máy làm Router.

Kiến trúc này gần giống với Screened Host trong trường hợp khi mà exterior/interior Router bị đột nhập vào thì lưu thông trong mạng bên trong sẽ bị lộ ra bên ngoài nhưng tốt hơn Screened Host đó là nó cũng sử dụng thêm một mạng bên ngoài. Mạng bên ngoài sẽ chứa các Server có thể nối ra Internet mà nếu các Server này bị đột nhập thì lưu thông của mạng bên trong cũng không bị lộ ra bên ngoài. Kiến trúc này cũng gần giống với Screened Subnet nhưng mà exterior Router và interior Router được ghép chung nên nó giảm đi số lớp bảo vệ. Nói chung, kiến trúc ghép chung interior Router và exterior Router ở trung gian giữa hai kiến trúc này.

**2.6. 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.



Hình 2.6: Kiến trúc ghép chung Bastion Host và Router ngoài.

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 do tốt 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**

Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router. Các phần mềm quản lí an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting). Một Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

* Bộ lọc gói (Packet-Filter)
* Cổng ứng dụng (Application-leved Gateway hay Proxy Server)
* Cổng mạch (Circuite level Gateway)

**3.1 Bộ lọc gói (Packet Filtering):**

**3.1.1 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 TCI/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, 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 được. 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).
* Dựa vào 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 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.

**3.1.2 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, vì 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 vể các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể có thể nhận trên mỗi trường. Khi đòi hỏi vể sự lọc càng lớn, các luật lệ vể 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.

**3.2. Cổng ứng dụng (Application-Level Gateway):**

**3.2.1 Nguyên lí 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 ngưòi 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 môt proxy đang có vấn để.

Ví dụ: Telnet Proxy

Ví dụ: Một người dùng bên ngoài (gọi là Outside Client) muốn sử dụng dịch vụ Telnet để kết nối vào hệ thống mạng qua một Bastion Host có Telnet Proxy. Quá trình xảy ra như sau:

1. Outside Client Telnet đến Bastion Host kiểm tra password, nếu hợp lệ thì Client được phép vào giao diện của Telnet Proxy. Telnet Proxy cho phép một tập nhỏ những lệnh của Telnet, và quyết định những máy chủ nội bộ nào Outside Client được phép truy nhập.
2. Outside Client chỉ ra máy chủ đích và Telnet Proxy tạo một kết nối của riêng nó tới máy chủ bên trong và chuyển các lệnh tới máy chủ dưới sự ủy quyền của outside Client. Outside Client thì tin rằng Telnet Proxy là máy chủ thật ở bên trong khi máy chủ ở bên trong thì tin rằng Telnet Proxy là Client thật.

**3.2.2 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.
* Cổng 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 filltering cho cổng 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 cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet.

**3.3. Cổng vòng (Circuit-level gateway) :**

Cổng vòng là một chức năng đặc biệt có thể thực hiện được bởi một cổng 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.

Hình minh họa một hành động sử dụng 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 ngoài (outside connection). Tuy nhiên vì sự kết nối này xuất hiện từ hệ thống Firewall, nó che dáu thông tin về mạng nội bộ.

Cổng vòng thường đưuọc sử dụng cho những kết nối ra ngoài, nơi mà các nhà quản trị mạng thật sự tin tưởng những người dùng bên trong. 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 bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp chức năng bức tường lửa để bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

**CHƯƠNG IV: GIẢI PHÁP TƯỜNG LỬA CHO DOANH NGHIỆP**

**4.1. Giới thiệu:**

Ngày nay việc sử dụng internet đã phổ biến gần như toàn bộ trong các doanh nghiệp. Đối với những ai chịu trách nhiệm quản lý hệ thống mạng máy tính cho tổ chức - doanh nghiệp trong môi trường kinh doanh hiện nay thì có lẽ bảo mật - an toàn dữ liệu là vấn đề hàng đầu trong mọi tình huống.

Một trong những công cụ hiệu quả nhất và cũng thông dụng nhất là sử dụng tường lửa (fire wall) nhằm kiểm soát sự truy cập từ bên ngoài vào mạng nội bộ và các giao dịch ra/vào mạng. Tuy nhiên, đầu tư cho một tường lửa khá tốn kém, nhất là đối với các tổ chức - doanh nghiệp vừa và nhỏ.

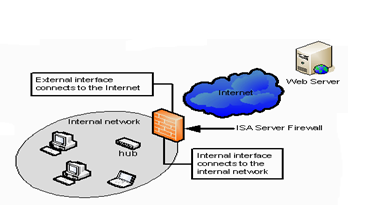
Trong trường hợp này, có lẽ giải pháp một thiết bị có thể xử lý mọi chức năng an toàn là hợp lý nhất. Thiết bị bảo mật 'Tất cả trong một' này phải đáp ứng yêu cầu về bảo mật - an toàn dữ liệu của tổ chức - doanh nghiệp một cách hiệu quả nhất mà không cần đến nhiều tầng thiết bị đắt tiền và phức tạp, cộng thêm một nhân viên chuyên trách.

Điều này quả thật rất cần thiết trong tình trạng Internet hiện nay đầy rẫy các mối đe dọa như sâu máy tính, chương trình phá hoại và ăn cắp thông tin, lỗ hổng bảo mật của các hệ điều hành và ứng dụng.

**4.2 Giải pháp firewall cho doanh nghiệp nhỏ:**

**4.2.1. ISA Server Enterprise 2000, ISA Server Enterprise 2004 :**

Đây là một phần mềm có các chức năng chính là :Bảo vệ mạng chống các cuộc tấn công từ Internet.



Hình 4.1: Mô hình triển khai SIA Server giữa Internal Network và Internet

* Cho phép các Client bên trong mạng nội bộ truy cập các dịch vụ ngoài Internet, có kiểm soát.
* Mô hình triển khai ISA Server giữa Internal Network và Internet

**4.2.2 Sonicwall PRO 2040:**

Firewall dành cho doanh nghiệp loại vừa này có thể đáp ứng mọi yêu cầu, dễ dàng nhận ra ngay điều này khi lấy thiết bị ra khỏi hộp, có thể đặt nó trên bàn, trên kệ tủ, hoặc lắp vào rack 1U đều được cả. SonicWALL Pro 2040 kết hợp hệ điều hành mở rộng SonicOS thế hệ mới của SonicWALL và một kiến trúc phần cứng có khả năng chịu tải tốt, miễn là cấu hình đúng, tất nhiên là không đơn giản.

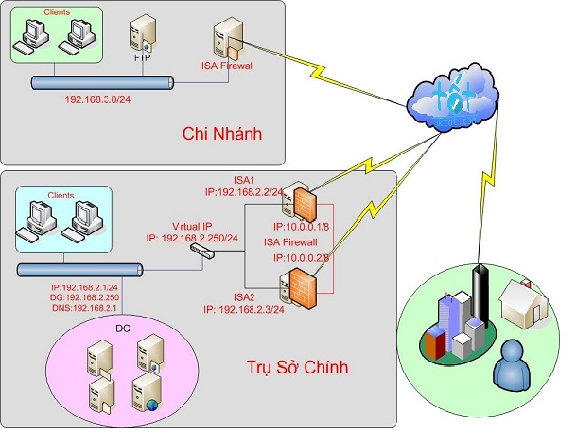
Khi sử dụng, người dùng phải cài đặt OS mở rộng của SonicWALL mới khai thác được nhiều tính năng cao cấp như kết nối đến nhiều ISP để dự phòng, cân bằng tải với các Pro 2040 khác, thiết lập NAT dựa theo chính sách và kết nối WAN dự phòng.

Mặc dù có thể vận hành Pro 2040 mà không cần hệ điều hành SonicOS Enhanced, nhưng phải cài hệ điều hành này thì mới có thể kích hoạt cổng giao tiếp thứ tư của thiết bị. Cổng này có chức năng của một cổng WAN, LAN, hay DMZ, hoặc nối sang một thiết bị Pro 2040 khác để dự phòng. SonicWall không hề thua kém các đối thủ, nó cũng tích hợp chức năng phòng chống virus và lọc nội dung.

Pro 2040 hoàn toàn làm vừa lòng, chẳng hạn, nó được trang bị một bộ xử lý chỉ làm mỗi nhiệm vụ mã hóa cho nên hiệu suất chẳng có gì khác biệt khi dùng chế độ mã hóa AES-256 hay 3DES. Hàng loạt cuộc tấn công giả lập cũng như ngăn chặn virus khi thử đều bị ngăn cản bởi Firewall này.

**4.3. Thiết lập một Firewall cho doanh nghiệp:**

Lựa chọn các giải pháp Firewall phần cứng hoặc Firewall phần mềm để xây dưng một Firewall cho doanh nghiệp.



Hình 4. Hình ảnh minh họa xây dựng hệ thống tường lửa doanh nghiệp

Việc thiết lập Firewall dựa vào các yếu tố sau:

**Trước hết cần xác định tài nguyên cần bảo vệ:**

* Máy trạm.
* Máy chủ.
* Các thiết bị mạng: Bộ định tuyến (Router), Getway, Repeater…
* Các máy chủ đầu cuối.
* Các chương trình phần mềm.
* Cáp mạng.
* Thông tin lưu trữ trong các tệp dữ liệu.

**Nghiên cứu các vấn đề sau:**

* Bảo vệ tài nguyên đó khỏi bị ai phá hoại.
* Xác suất của nguy cơ đe doạ.
* Mức độ quan trọng của nguồn tài nguyên.
* Các biện pháp có thể thực hiện để bảo vệ tài nguyên với thời gian nhanh nhất, đỡ tốn kém nhất.
* Kiểm tra chính sách an ninh mạng định kì.

**Nhận dạng các mối đe doạ:**

* Truy cập trái phép: Nói chung việc sử dụng bất cứ tài nguyên nào mà không được sự cho phép trước đều bị coi là truy cập trái phép.
* Nguy cơ để lộ thông tin: Việc để lộ thông tin cũng là một mối đe doạ. Cần phải xác định rõ các giá trị hay độ nhạy cảm của thông tin lưu trữ trên máy. Ở mức hệ thống việc để lọt mật khẩu truy nhập hệ thống có thể tạo thuận lợi cho việc truy nhập trái phép trong tương lai.
* Từ chối dịch vụ: Các mạng dùng để kết nối các nguồn tài nguyên có giá trị như các máy tính và các cơ sở dữ liệu cung cấp các dịch vụ mà một cơ quan dựa vào. Nếu các dịch vụ này không sẵn sàng sẽ dẫn đến ảnh hưởng công việc kinh doanh của đơn vị. Rất khó có thể đoán trước được hình thức từ chối dịch vụ, dưới đây liệt kê một số ví dụ về từ chối dịch vụ:
  + - Hệ thống máy bị dừng vì một gói tin của kẻ phá hoại.
    - Mạng bị dừng vì bị tràn lưu lượng.
    - Các thiết bị bảo vệ mạng bị phá hỏng….
* Các điểm truy nhập: Điểm truy nhập mà ở đó những người sử dụng trái phép đi vào hệ thống. Nếu ta có càng nhiều điểm truy nhập thì càng làm tăng nguy cơ cho mạng.
* Các hệ thống có cấu hình không đúng: Những kẻ đột nhập vào mạng chúng thường cố gắng phá hoại các máy chủ trên mạng. Các máy tính chủ đóng vai trò như các Server của Telnet là các mục tiêu rất phổ biến. Nếu máy tính chủ không được cấu hình một cách đúng đắn thì hệ thống sẽ rất dễ bị phá hoại.
* Virus: Khi độ phức tạp của phần mềm tăng lên thì độ phức tạp của Virus trong bất kì hệ thông nào cũng tăng. Có lẽ sẽ không có phần mềm nào mà không bị nhiễm Virus. Các Virus an toàn được biết đến một cách rộng rãi cũng là các phương pháp phổ biến để truy nhập trái phép. Nếu việc cài đặt hệ thống là mở và được biết đến một cách rộng rãi thì kẻ đột nhập có thể sử dụng những điểm yếu của chương trình chạy ở chế độ ưu tiên để truy nhập hệ thống ở chế độ đặc quyền.
* Các mối đe doạ từ bên ngoài: Những người trong cuộc thường truy nhập trực tiếp phần mềm máy tính mạng nhiều hơn so với phần cứng. Nếu như một người trong cuộc quyết định phá hoại thì người đó tạo ra mối đe doạ đáng kể cho an toàn của mạng. Nếu người đó tiếp cận dễ dàng với hệ thống thì hệ thống càng dễ bị phá hoại hơn. Người phá hoại có thể dễ dàng chạy bộ giải mã giao thức và nắm bắt phần mềm để phân tích lưu lượng của giao thức. Hầu hết các ứng dụng TCP/IP (Telnet, FTP) chỉ có cơ chế xác minh rất yếu trong đó mật khẩu được chuyển đi dưới dạng văn bản rõ nghĩa.
* An toàn vật lý: Nếu bản thân máy tính không được an toàn về mặt vật lý thì các cơ chế an toàn phần mềm có thể dễ dàng bị bỏ qua. Trong trường hợp các máy trạm DOS, WINDOWS đều không có cơ chế bảo vệ phần mềm. Đối với hệ điều hành Unix không có người quản lý thì các ổ đĩa vật lý có thể bị đánh tráo, hoặc nếu ta để hệ thống này trong chế độ đặc quyền thì máy trạm coi như bị bỏ ngỏ. Nói cách khác kẻ đột nhập có thể tạm dừng máy tính này lại và đưa nó trở lại chế độ ưu đãi rồi sau đó lấy các chương trình Trojan-hores vào hoặc có thể thực hiện các hành động khác nhằm làm cho hệ thống trở nên rộng mở cho các vụ tấn công trong tương lai.

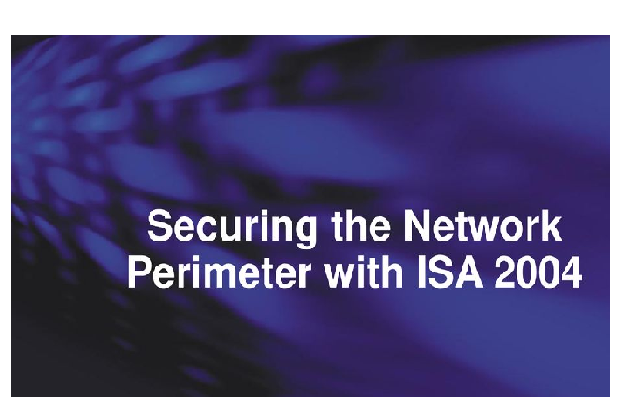
**4.4 Cài đặt cấu hình Firewall :**

Sau đây sẽ tiến hành cài đặt một Firewall cho doanh nghiệp bằng phần mềm **ISA Server 2004 Firewall**

**4.4.1 Tìm hiểu về phần mềm ISA Server 2004 Firewall :**

Trong số những sản phẩm tường lửa (firewall) trên thị trường hiện nay thì ISA Server 2004 của Microsoft được nhiều người yêu thích do khả năng bảo vệ hệ thống mạnh mẽ cùng với cơ chế quản lý linh hoạt. ISA Server 2004 Firewall có hai phiên bản Standard và Enterprise phục vụ cho những môi trường khác nhau.

ISA Server 2004 Standard đáp ứng nhu cầu bảo vệ và chia sẻ băng thông cho các công ty có quy mô trung bình. Với phiên bản này có thể xây dựng Firewall để kiểm soát các luồng dữ liệu vào và ra hệ thống mạng nội bộ của công ty, kiểm soát quá trình truy cập của người dùng theo giao thức, thời gian và nội dung nhằm ngăn chặn việc kết nối vào những trang web có nội dung không thích hợp. Bên cạnh đó còn có thể triển khai hệ thống VPN Site to Site hay Remote Access hỗ trợ cho việc truy cập từ xa, hoặc trao đổi dữ liệu giữa các văn phòng chi nhánh. Đối với các công ty có những hệ thống máy chủ quan trọng như Mail Server, Web Server cần được bảo vệ chặt chẽ trong một môi trường riêng biệt thì ISA 2004 cho phép triển khai các vùng DMZ (thuật ngữ chỉ vùng phi quân sự) ngăn ngừa sự tương tác trực tiếp giữa người bên trong và bên ngoài hệ thống. Ngoài các tính năng bảo mật thông tin trên, ISA 2004 còn có hệ thống đệm (cache) giúp kết nối Internet nhanh hơn do thông tin trang web có thể được lưu sẵn trên RAM hay đĩa cứng, giúp tiết kiệm đáng kể băng thông hệ thống. Chính vì lý do đó mà sản phẩm Firewall này có tên gọi là Internet Security & Aceleration (bảo mật và tăng tốc Internet).



Hình 4. : Hình ảnh giao diện của ISA 2004

ISA Server 2004 Enterprise được sử dụng trong các mô hình mạng lớn, đáp ứng nhiều yêu cầu truy xuất của người dùng bên trong và ngoài hệ thống. Ngoài những tính năng đã có trên ISA Server 2004 Standard, bản Enterprise còn cho phép thiết lập hệ thống mảng các ISA Server cùng sử dụng một chính sách, điều này giúp dễ dàng quản lý và cung cấp tính năng Load Balancing (cân bằng tải).

**4.4.2. Các tính năng trên ISA 2004**

ISA Server 2004 được thiết kế để bảo vệ Network, chống các xâm nhập từ bên ngoài lẫn kiểm soát các truy cập từ bên trong Nội bộ Network của một Tổ chức. ISA Server 2004 Firewall làm điều này thông qua cơ chế điều khiển những gì có thể được phép qua Firewall và những gì sẽ bị ngăn chặn. Chúng ta hình dung đơn giản như sau: Có một quy tắc được áp đặt trên Firewall cho phép thông tin được truyền qua Firewall, sau đó những thông tin này sẽ được “Pass” qua, và ngược lại nếu không có bất kì quy tắc nào cho phép những thông tin ấy truyền qua, những thông tin này sẽ bị Firewall chặn lại.

ISA Server 2004 Firewall chứa nhiều tính năng mà các Security Admin có thể dùng để đảm bảo an toàn cho việc truy cập Internet, và cũng bảo đảm an ninh cho các tài nguyên trong Nội bộ Network . Cuốn sách cung cấp cho các Security Admin hiểu được những khái niệm tổng quát và dùng những tính năng phổ biến, đặc thù nhất trên ISA Server 2004, thông qua những bước hướng dẫn cụ thể (Steps by Steps).

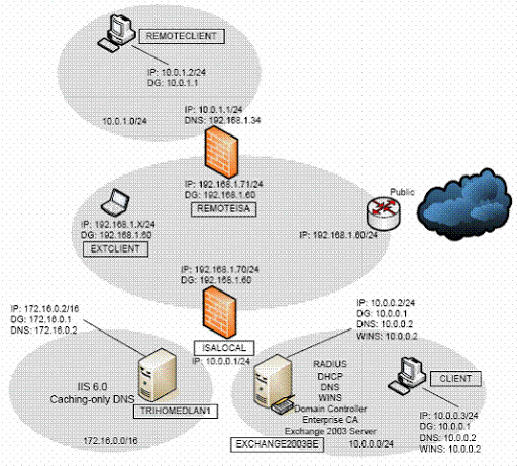
Firewalls không làm việc trong một môi trường “chân không”, vì đơn giản là chúng ta triển khai Firewall để bảo vệ một cái gì đó, có thể là một PC, một Server hay cả một hệ thống Network với nhiều Service được triển khai như Web, Mail, Database…

**4.4.3 Cài đặt ISA Server**

**Yêu cầu cài đặt:** ISA 2004 phải được cài đặt trên nền phần cứng và phần mềm như sau:

* Phần cứng tối thiểu:
* CPU: 500MHz.
* RAM: 256MB.
* Hard Disk: phân vùng NTFS, >=150MB dung lượng còn trống.
* Máy có 2 card mạng.
* Phần mềm:
* Windows 2000 server, SP4.
* Windows 2003 server.

Sau khi đã thiết lập đầy đủ các thông tin cần thiết, tiến hành cài đặt ISA Server 2004 Standard trên máy tính dùng làm Firewall.



Hình 4. : Mô hình Network Lap -7Computer

**Bước 1**: Chạy file setup và click vào **Install ISA Server 2004**

**Bước 2**: Trong hộp thoại **Microsoft ISA Server 2004 - Installation Wizard**, ta click **Next**.

**Bước 3**: Sau đó ta chọn **I accept the terms in the license agreement** và sau đó click **Next**.

**Bước 4**: Ta điền đầy đủ thông tin và số serial vào rồi click **Next**.

**Bước 5**: Ta chọn cài đặt chế độ **Custom** rồi click **Next**.

**Bước 6**: Mặc định chỉ có hai dịch vụ **Firewall Services** và **ISA Server Management**, ta chọn thêm **Firewall Client Installation Share**. Rồi click **Next**.

**Bước 7**: Ta sẽ click vào **Add**

**Bước 8**: Ta sẽ cung cấp dãy địa chỉ IP chứa các máy tính trong mạng nội bộ (From, To). Lưu ý, dãy địa chỉ này phải chứa IP của giao tiếp mạng Inside. Rồi click **Add**. Sau đó **OK.**

**Bước 9**: Trong hộp thoại **Internal Network** ta click **Next.**

**Bước 10**: Ta chọn **Allow computers running earlier version of Firewall Client software to connect**. Rồi chọn **Next**.

**Bước 11**: Trong hộp thoại **Services** ta click **Next**.

**Bước 12**: Trong hộp thoại **Ready to Install the Program** ta click **Install**. Sau đó quá trình cài đặt sẽ bắt đầu. Xong thì ta bấm **Finish** để hoàn tất.

**TỔNG KẾT**

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 dữ liệu khác.

# 