**BÁO CÁO ĐỒ ÁN**

**AN TOÀN MÁY CHỦ WINDOWS**



**Đề tài: Tìm hiểu và cài đặt hệ thống Firewall ISA**

|  |  |
| --- | --- |
|  |  |

Thành phố Hồ Chí Minh, năm 2022

**MỤC LỤC**

[LỜI MỞ ĐẦU 1](#_Toc106962011)

[CHƯƠNG 1 TỔNG QUAN 2](#_Toc106962012)

[1.1. Tổng quan đề tài 2](#_Toc106962013)

[1.1.1 Khảo sát thực trạng 2](#_Toc106962014)

[1.2.1 Đánh giá 2](#_Toc106962015)

[1.2. Mục tiêu 3](#_Toc106962016)

[1.3. Cấu trúc đề tài 3](#_Toc106962017)

[CHƯƠNG 2 CƠ SỞ LÝ THUYẾT 4](#_Toc106962018)

[2.1. Giới thiệu về hệ thống FireWall ISA 4](#_Toc106962019)

[2.2. Phân loại FireWall 5](#_Toc106962020)

[2.3. Nhiệm vụ chính của FireWall 6](#_Toc106962021)

[2.4. Firewall hoạt động như thế nào? 7](#_Toc106962022)

[2.5. Liệu firewall có đủ để ngăn chặn sự xâm nhập không ? 8](#_Toc106962023)

[2.6. Sản phẩm Firewall được ứng dụng trong thực tế 8](#_Toc106962024)

[2.7. ISA Server là gì? 10](#_Toc106962025)

[2.7.1 Các công nghệ cho các dịch vụ của ISA server là gì? 11](#_Toc106962026)

[2.7.2. Ưu điểm của ISA server 12](#_Toc106962027)

[2.7.3. Cách cài đặt cấu hình ISA server 13](#_Toc106962028)

[2.7.4 Cơ chế hoạt động của ISA Server 13](#_Toc106962029)

[2.7.6 Các mô hình triển khai của ISA Server 16](#_Toc106962030)

[2.7.7. ISA Server bảo mật truy cập Internet 18](#_Toc106962031)

[2.8. ISA Client là gì? 19](#_Toc106962032)

[2.8.1. Triển khải Firewall Client 19](#_Toc106962033)

[2.8.2. Firewall Client làm việc như thế nào 19](#_Toc106962034)

[2.8.3. Ứng dụng của ISA Client 20](#_Toc106962035)

[2.8.4. Ưu điểm và Ý nghĩa của Firewall client 21](#_Toc106962036)

[2.8.5. Cảnh báo bảo mật ISA FIREWALL 24](#_Toc106962037)

[2.8.6. Một số cách phòng chống tấn công 24](#_Toc106962038)

[2.8.7. Khả năng kết nối VPN 25](#_Toc106962039)

[2.8.8. Về khả năng quản lý 25](#_Toc106962040)

[2.8.9. Nhiệm vụ bảo mật SSL. 26](#_Toc106962041)

[CHƯƠNG 3 KẾT QUẢ THỰC NGHIỆM 28](#_Toc106962042)

[3.4. Các bước thực hiện 29](#_Toc106962043)

[3.4.1. Cài đặt ISA Server 2006 29](#_Toc106962044)

[3.4.2. Cấu hình Access Rule trên máy ISA 33](#_Toc106962045)

[CHƯƠNG 4 KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 35](#_Toc106962046)

[4.1. Kết luận 35](#_Toc106962047)

[4.2. Hướng phát triển 35](#_Toc106962048)

[TÀI LIỆU KHAM KHẢO 36](#_Toc106962049)

**MỤC LỤC HÌNH ẢNH**

[Hình 2.1: Hình ảnh tường lửa 4](#_Toc106961972)

[Hình 2.2: Hình các loại firewall 6](#_Toc106961973)

[Hình 2.3: Software Firewalls 9](#_Toc106961974)

[Hình 2.4: Appliance Firewalls 9](#_Toc106961975)

[Hình 2.5: Hoạt động của ISA server 12](#_Toc106961976)

[Hình 2.6: Hệ thống tường lửa bảo mật chắc chắn của ISA server 12](#_Toc106961977)

[Hình 2.7: Mô hinh ISA đơn giản 14](#_Toc106961978)

[Hình 2.8: Mô hình Bastion-Host 16](#_Toc106961979)

[Hình 2.9: Mô hình Three-home 18](#_Toc106961980)

[Hình 2.10: Các kết nối Firewall client vào ISA 2004 21](#_Toc106961981)

[Hình 3.2: Cấu hình Access Rule trên máy ISA 33](#_Toc106961982)

[Hình 3.3: Cấu hình những trang Web được và không được truy cập 33](#_Toc106961983)

[Hình 3.4: Cấu hình Access Rule cho phép máy ISA truy cập mạng 34](#_Toc106961984)

# LỜI MỞ ĐẦU

Công nghệ thông tin là một trong những ngành đang rất được trọng dụng trong những năm gần đây, với sự tác động mạnh mẽ của cách mạng công nghệp 4.0 ngành công nghệ thông tin đang là mối quan tâm hàng đầu trong bước tiến mới của thời đại công nghệ hóa đang dần thay thế phần lớn công việc của con người. Thế nên ở các nước đang đẩy mạnh đào tạo ra các nguồn nhân lực Công nghệ thông tin nhằm đáp ứng nhu cầu việc làm mà xã hội cần thiết để đảm bảo nguồn nhân lực cho sự phát triển của thời đại công nghệ này.

Gửi thư là một hình thức trao đổi thông tin gián tiếp bằng chữ viết (có thể có thêm hình ảnh, ký tự hoặc vật dụng đính kèm) giữa người viết thư và người nhận thư (đọc, xem thư) thông qua trung gian là người đưa thư. Tuy nhiên phương pháp này rất tốn thời gian và bất tiện cho người viết phải chuẩn bị dụng cụ và chi phí để soạn ra một lá thư và người nhận phải chờ đợi trong thời gian dài mới có thể nhận và đọc được thư. Vì thế, gửi thư điện tử là phần mềm giúp người dùng giảm được thời gian và chi phí, tiện lợi và có thể gửi đi bất cứ lúc nào.

Gửi thư điện tử là công việc hầu hết người dùng máy tính hoặc điện thoại đều sử dụng hiện nay. Trong quá trình gửi đi sẽ có những vấn đề rủi ro phát sinh như thư không gửi được, bị đánh cắp, nội dung bị thay đổi bởi virus từ những tay hacker. Vì thế mà ta cần tính năng bảo mật cho việc gửi thư điện tử cũng như đảm bảo cho quá trình gửi thư được an toàn, không bị gián đoạn hoặc lấy cắp.

Trong tài liệu này sẽ đề cập cho các bạn cách thiết lập bảo mật cho việc gửi thư điện tử. Mong rằng, qua tài liệu này có thể gợi ý cho các bạn về công việc sau này và giúp bạn tự tin vạch ra những bước đi đúng đắn, quyết định sang suốt trước ngưỡng cửa lựa chọn nghề nghiệp của mình.

# TỔNG QUAN

## Tổng quan đề tài

### Khảo sát thực trạng

- Trong năm 2008, Symantec đã phát hiện 55.389 máy chủ đặt website lừa đảo, tăng 60% so với con số 33.428 của năm 2007. Những lừa đảo liên quan đến các dich vụ chính chiếm với 76% các vụ lừa đảo năm 2008, tăng mạnh so với con số 52% năm 2007.

-90% những mối đe dọa bảo mật được phát hiện bởi Symantec trong giai đoạn nghiên cứu này đều chú trọng vào ăn cắp những thông tin trên quan trọng. Những đe dọa về khả năng nhờ bàn phím, được dùng để ăn cắp thông tin như những thông tin tài khoản ngân hàng trực tuyến – chiếm 76% tổng các mối đe dọa nhắm tới thông tin quan trọng, tăng so với con số 72% trong năm 2007.

### Đánh giá

* Ưu điểm:

+ Gửi và nhận thư nhanh hơn so với cách gửi thư truyền thống

+ Có thể gửi đi bất cứ lúc nào

+ Có thể sử dụng trình duyệt hoặc mạng internet bất kỳ để gửi

+ Có thể gửi cho một hoặc nhiều người cùng lúc

* Nhược điểm:

+ Người nhận cần truy cập internet để nhận thư

+ Virus có thể phát tán từ internet vào các tập tin đính kèm trong thư từ những tay hacker

+ Những chiêu thức lừa đảo được thực hiện rất tinh vi nếu không cẩn thận có thể bị đánh cắp danh tính hoặc mất tiền.

+ Đôi khi thư được gửi lại đi vào thư rác của hệ thống.

**-** Từ các vấn đề trên, ta cần phải xây dựng hệ thống mới có yêu cầu kỹ thuật, quản lý chuyên nghiệp, tính bảo mật cao, giải quyết các khuyết điểm của hệ thống cũ.

## Mục tiêu

- Nghiên cứu, tìm hiểu các chức năng, hoạt động của các dịch vụ trên hệ thống Firewall ISA

- Nghiên cứu cách thức hoạt động, các yêu cầu, công nghệ sử dụng dịch vụ để thực hiện giao dịch

- Nghiên cứu cách cài đặt các dịch vụ bảo mật

- Nâng cao tầm hiểu biết và mở rộng kiến thức

- Rèn luyện kỹ năng làm việc nhóm, cách triển khai của một dự án

- Học hỏi những công nghệ mới, áp dụng công nghệ vào một dự án cụ thể

## Cấu trúc đề tài

Đồ án được chia làm 4 phần tương ứng với 4 chương:

* Chương 1: Tổng quan

+ Tổng quan đề tài

+ Mục tiêu

+ Cấu trúc đề tài

* Chương 2: Cơ sở lý thuyết

+ Firewall

+ Firewall Server

+ Firewall Client

+ Khả năng kết nối VPN

* Chương 3: Kết quả thực nghiệm

+ Kịch bản thực nghiệm

+ Yêu cầu thực nghiệm

+ Công cụ sử dụng

+ Các bước thực hiện

* Chương 4: Kết luận và hướng phát triển

# CƠ SỞ LÝ THUYẾT

## 2.1. Giới thiệu về hệ thống FireWall ISA

Tường lửa (Firewall) là một hệ thống an ninh mạng nhằm ngăn chặn việc truy cập dữ liệu trái phép, bảo vệ nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống.

Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Nó kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Nghĩa là, chỉ những traffic phù hợp với chính sách được định nghĩa trong tường lửa mới được truy cập vào mạng, mọi traffic khác đều bị từ chối.



Hình 2.1: Hình ảnh tường lửa

Bất kì máy tính nào kết nối tới Internet cũng cần có firewall, giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng. Việc có một “người gác cổng” như vậy để giám sát mọi việc xảy ra rất quan trọng bởi 2 lý do:

* Thứ nhất, bất kì máy tính kết nối mạng nào thường kết nối vĩnh viễn với Internet.
* Thứ hai, mỗi máy tính trực tuyến lại có một chữ ký điện tử riêng, được gọi là Internet Protocol address (hay còn gọi là địa chỉ IP): Nếu không có firewall hỗ trợ, nó chẳng khác gì chuyện bạn bật tất cả đèn lên và mở rộng cửa để đón trộm vào.

## 2.2. Phân loại FireWall

**\* Firewall hoạt động dựa trên 2 loại:**

- Personal Firewall: được thiết kế với tính năng bảo vệ máy tính trước sự xâm nhập trái phép từ bên ngoài vào.

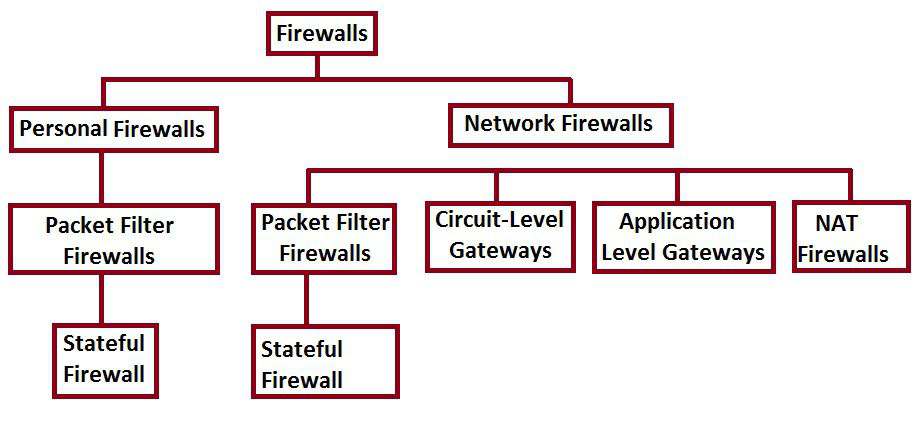
- Bên cạnh đó thì Personal Firewall còn được tích hợp thêm tính năng như theo dõi các phần mềm chống virus, phần mềm chống xâm nhập để bảo vệ dữ liệu. Một số Personal Firewall thông dụng như: Microsoft Internet connection firewall, Symantec personal firewall, Cisco Security Agent….Loại Firewall này thì thích hợp với cá nhân bởi vì thông thường họ chỉ cần bảo vệ máy tính của họ, thường được tích hợp sẵn trong máy tính Laptop, máy tính PC..

- Network Firewall:được thiết kế để bảo vệ các host trong mạng trước sự tấn công từ bên ngoài. Có các Appliance – Based network Firewalls như Microsoft ISA Server, Linux-Based IPTables.

- Sự khác nhau giữa hai loại Firewall này là số lượng host được Firewall bảo vệ. Bởi Personal Firewall chỉ bảo vệ một máy tính duy tính nhất còn Network Firewall thì khác, nó sẽ bảo vệ hết hệ thống mạng máy tính.

- Bên cạnh đó Network Firewall được cấu tạo bởi các thành phần chính:

* Bộ lọc Packet (Packet- Filtering Router)
* Cổng ứng dụng ( đó là Application-Level Gateway hay Proxy Server).
* Cổng mạch (Circuite Level Gateway).



Hình 2.2: Hình các loại firewall

## 2.3. Nhiệm vụ chính của FireWall

**+ Đóng vai là một bức tường kiểm soát việc ra vào của các gói tin. Thì phải firewall phải thực hiện những nhiệm vụ:**

* Cho phép hoặc vô hiệu hóa các dịch vụ truy cập ra bên ngoài, đảm bảo thông tin chỉ có trong mạng nội bộ.
* Cho phép hoặc vô hiệu hóa các dịch vụ bên ngoài truy cập vào trong.
* Phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài.
* Hỗ trợ kiểm soát địa chỉ truy cập (bạn có thể đặt lệnh cấm hoặc là cho phép).
* Kiểm soát truy cập của người dùng.
* Hỗ trợ kiểm soát nội dung thông tin và gói tin lưu chuyển trên hệ thống mạng.
* Lọc các gói tin dựa vào địa chỉ nguồn, địa chỉ đích và số Port ( hay còn cổng), giao thức mạng.
* Người quản trị có thể biết được kẻ nào đang cố gắng để truy cập vào hệ thống mạng.
* Bảo vệ tài nguyên của hệ thống bởi các mối đe dọa bảo mật.
* Cân bằng tải: Bạn có thể sử dụng nhiều đường truyền internet cùng một lúc, việc chia tải sẽ giúp đường truyền internet ổn định hơn rất nhiều.
* Tính năng lọc ứng dụng cho phép ngăn chặn một số ứng dụng mà bạn muốn. Ví dụ như Facebook Messenger, Skype, Zalo…

## 2.4. Firewall hoạt động như thế nào?

- Khi một gói tin được chuyển tải trên mạng, nó được chia nhỏ thành các gói (packet). Mỗi gói sẽ được gán một địa chỉ để có thể đến đích, sau đó được nhận dạng và tái lập lại ở đích. Các địa chỉ được lưu trong phần đầu của gói tin (header) và Firewall sẽ dựa vào Header của gói tin để lọc.

- Bộ lọc gói tin có khả năng cho phép hay từ chối mỗi gói tin mà nó nhận được. Nó kiểm tra toàn bộ đọan dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong số các luật của lọc gói tin hay không. Các luật lọc gói tin này sẽ dựa trên các thông tin ở đầu mỗi gói tin (Header), Header của gói tin bao gồm các thông tin như sau:

* Version: Phiên bản của IP, hiện tại chúng ta đang sử dụng IP phiên bản 4 (Ipv4).

– IP Header Length: Độ dài của IP header là 32 bits.

– Type of Service (ToS): Loại dịch vụ.

– Size of Datagram: Kích thước của gói tin được tính bằng byte, bao gồm kích thước của Header và kích thước của Data (dữ liệu).

– Identification: Dấu hiện nhận dạng, trường hợp này được sử dụng để lắp ghép các phân đoạn khi tất cả các gói tin đã đến đích.

– Flag: Là một trong ba cờ được sử dụng để điều khiển, định tuyến cho một gói tin và báo cho người nhận biết gói tin có bao nhiêu phần.- Time To Live: Chỉ ra số lượng Hops hoặc liên kết mà gói tin có thể đi qua và được sử dụng để tránh quá trình lặp lại của gói tin (tránh cho gói tin chạy vô hạn).

– Protocol: Giao thức truyền tin (TCP, UDP, ICMP, …

– Header Checksum: Mục này được sử dụng để kiểm tra xem tổng số gói tin mà người gởi có bằng tổng số gói tin mà người nhận nhận được không. Nếu không bằng nhau, nó sẽ báo lỗi và yêu cầu người gởi gởi lại (nếu sử dụng giao thức TCP); ngược lại, nó sẽ hủy gói tin nếu sử dụng giao thức UDP.

– Source Address: Địa chỉ nơi xuất phát.

– Destination Address: Địa chỉ nơi nhận.

– Source port: Cổng nguồn.

– Destination port: Cổng đích.

– Options: Tùy chọn này không được sử dụng.

+ Nếu gói tin thỏa các luật đã được thiết lập trước của Firewall, gói tin đó được chuyển qua, ngược lại, gói tin sẽ bị hủy. Việc kiểm soát các cổng sẽ cho phép Firewall kiểm soát một số loại kết nối nhất định mới được vào mạng cục bộ.

+ Do việc kiểm tra dựa trên Header của các gói tin nên bộ lọc không kiểm soát được nội dung thông tin của gói tin đó. Vì vậy các gói tin chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá họai của Hacker.

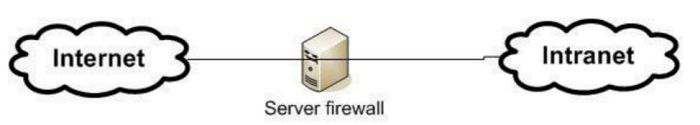
## 2.5. Liệu firewall có đủ để ngăn chặn sự xâm nhập không ?

- Có cách nào để ngăn chặn hoạt động phá hoại của các thành phần xấu. Nếu có một firewall không có đủ hay không? Bạn có thể download phần mềm firewall miễn phí nào đó và cài đặt nó để sử dụng song song cùng firewall của Windows hoặc kích hoạt firewall phần cứng được tích hợp sẵn trong router. Firewall thiết kế ra để nhằm cách ly những mối nguy hại ở bên ngoài và bảo vệ  tất cả các thiết bị, máy tính kết nối tới mạng gia đình.

- Hầu như các loại router đều được quản lý qua một màn hình cấu hình dựa trên trình duyệt web. Có thể tìm địa chỉ bằng cách kiểm tra sách hướng dẫn.

## 2.6. Sản phẩm Firewall được ứng dụng trong thực tế

- Software Firewalls: Hay còn gọi là Firewall mềm, đây là loại Firewall được tích hợp trên hệ điều hành, nó bao gồm các sản phẩm như: SunScreen firewall, Check Point NG, IPF, Linux’s IPTables, Microsoft ISA server …



Hình 2.3: Software Firewalls

* **Firewall được cài đặt trên Server:**

**+ Ưu điểm:**

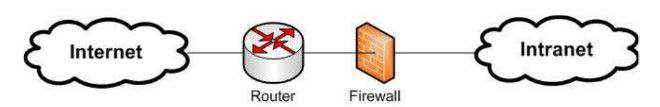
* Firewall mềm thường đảm nhận nhiều vai trò hơn firewall cứng, nó có thể đóng vai trò như một DNS server hay một DHCP server.
* Việc thay đổi và nâng cấp thiết bị phần cứng là tương đối dễ dàng và nhanh chóng.

**+ Nhược điểm:**

* Firewall mềm được cài đặt trên một hệ điều hành do đó không thể loại trừ khả năng có lỗ hổng trên hệ điều hành đó được. Khi lỗ hổng được phát hiện và bạn thực hiện cập nhật bản vá lỗi cho hệ điều hành đó thì bạn nên nâng cấp bản vá cho Firewall luôn, nếu không rất có thể Firewall sẽ hoạt động không ổn định
* Firewall mềm thường có hiệu suất thấp hơn Firewall cứng.

**\* Appliance Firewalls:**

- Hay còn gọi là Firewall cứng. Đây là loại Firewall cứng được tích hợp sẵn trên các phần cứng chuyên dụng, thiết kề này dành riêng cho Firewall. Một số Firewall cứng như Cisco PIX, WatchGuard Fireboxes, NetScreen firewall, SonicWall Appliaces, Nokia firewall…



Hình 2.4: Appliance Firewalls

* **Trường hợp Firewall được tích hợp trên Router**

**+ Ưu điểm:**

* Cung cấp hiệu suất tổng thể tốt hơn so với Firewall mềm vì hệ điều hành của firewall cứng được thiết kế để tối ưu cho firewall.
* Tính bảo mật cao hơn và tổng chi phí thấp hơn so với Firewall mềm.

**+ Nhược điểm:**

* Nó không được linh hoạt như Firewall mềm. Bạn sẽ không thể nào mà tích hợp thêm các chức năng và quy tắc như trên firewall mềm được. Ví dụ như chức năng kiểm soát thư rác đối với firewall mềm thì bạn chỉ cần cài đặt chức năng này như một ứng dụng, nhưng đối với Firewall cứng thì đòi hỏi bạn phải có thiết bị phần cứng hỗ trợ cho chức năng này.

**\* Integrated firewalls:**

- Hay còn gọi là Firewall tích hợp. Ngoài chức năng cơ bản của Firewall ra thì nó còn đảm nhận các chức năng khác ví dụ như VPN, phát hiện và chống xâm nhập từ bên ngoài, lọc thư rác, chống lại virus…

**+ Ưu điểm:**

* Sử dụng 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.

**+ Nhược điểm:**

* Ưu điểm thì là như vậy, tuy nhiên việc tích hợp nhiều chức năng trên cùng một thiết bị sẽ dẫn đến việc khó khăn hơn trong khắc phục sự cố.
* Trên đây là toàn bộ những thông tin cơ bản về Firewall, thiết bị tường lửa không thể thiếu trong các hệ thống mạng doanh nghiệp hiện nay.

## 2.7. ISA Server là gì?

- ISA server là một thành viên của máy chủ doanh nghiệp .NET. Nó xuất hiện ở cả phiên bản tiêu chuẩn và doanh nghiệp. Mặc dù phiên bản tiêu chuẩn có thể được sử dụng như một máy chủ độc lập (hỗ trợ tối đa bốn bộ xử lý) cho các tổ chức có quyền truy cập Internet thấp hơn, phiên bản doanh nghiệp được sử dụng để triển khai ở quy mô lớn do các chức năng bổ sung của nó.

- Máy chủ tăng tốc và bảo mật Internet (máy chủ ISA) là một máy chủ cung cấp tường lửa tổ chức và giải pháp bộ nhớ cache Web cho Windows cùng với kết nối Internet an toàn, nhanh chóng và dễ quản lý.

- ISA giúp thực hiện chính sách bảo mật doanh nghiệp của tổ chức thông qua các công cụ quản trị của nó, giúp điều chỉnh việc sử dụng dựa trên các tiêu chí nhóm, ứng dụng, đích, lịch biểu và nội dung của người dùng.

- Nền tảng mở rộng của nó cung cấp khả năng dự phòng phần cứng và cân bằng tải và cho phép sử dụng hiệu quả tài nguyên mạng thông qua các cơ chế bộ nhớ đệm phức tạp của nó.

### 2.7.1 Các công nghệ cho các dịch vụ của ISA server là gì?

Dịch vụ Microsoft Firewall để giám sát tất cả lưu lượng cấp gói, cấp mạch và cấp ứng dụng.

Một proxy Web để lưu trữ và phục vụ nội dung Web truy cập thường xuyên để giảm lưu lượng mạng và cung cấp truy cập nhanh hơn vào các trang Web thường xuyên truy cập.

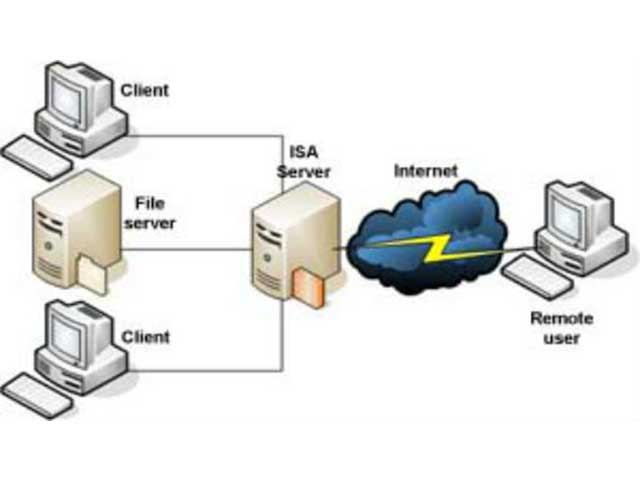
Dịch địa chỉ mạng an toàn để cung cấp sự minh bạch địa chỉ cho các khách hàng được kết nối mạng.

Bộ nhớ đệm RAM và Giao thức định tuyến bộ nhớ cache cho bộ nhớ đệm nâng cao.

Bộ lọc gói giao thức Internet động chỉ mở cổng khi cần thiết, do đó giảm nguy cơ tấn công từ bên ngoài.

Mạng riêng ảo để đóng gói dữ liệu cá nhân qua mạng công cộng.

Thông báo để thông báo cho quản trị viên về sự kiện mạng đáng ngờ.

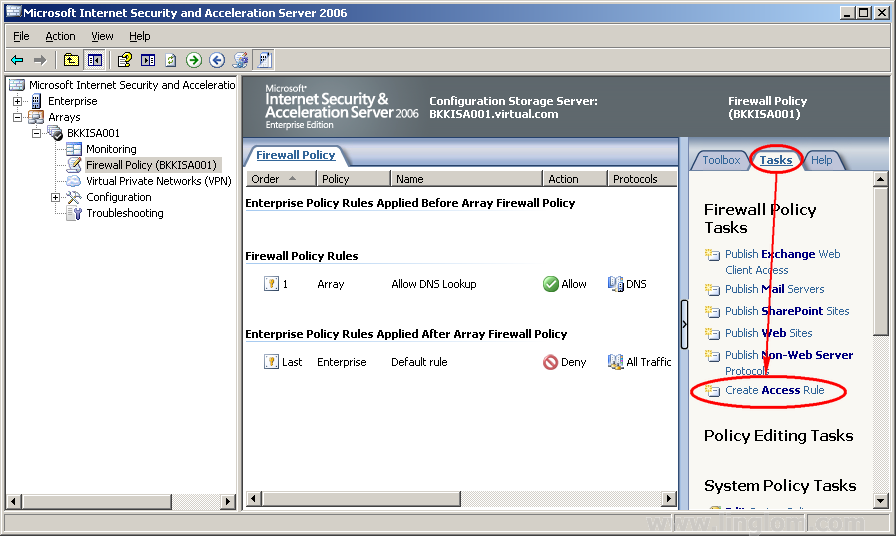


Hình 2.5: Hoạt động của ISA server

### 2.7.2. Ưu điểm của ISA server

Được bảo vệ bởi hệ thống tường lửa – Fire wall trong khi kết nối Internet. Tránh tối đa sự xâm phạm từ các đối tượng như hacker, virus,…

Với các tổ chức, doanh nghiệp, mọi dữ liệu thông tin cần được bảo mật ở mức tuyệt đối. Với máy các nhân lộ thông tin người dùng đã gây khó chịu thì với doanh nghiệp thì sẽ là những tổn thất về mặt tài sản, còn có thể là cả uy tín nữa.



Hình 2.6: Hệ thống tường lửa bảo mật chắc chắn của ISA server

### 2.7.3. Cách cài đặt cấu hình ISA server

- Bước 1: Tải phần mềm ISA server

Sau đó bạn chạy phần mềm, bảng cài đặt chọn Install ISA server

- Bước 2: Chọn Next, sau đó là “I accept the terms in the license agreement” và tiếp tục ấn Next

- Bước 3: Điền đầy đủ thông tin về User Name, Organization. Sau đó chọn Next

Nếu bạn vẫn đang loay hoay về vấn đề làm cách nào để đăng ký vps free không cần visa thì không nên bỏ qua thông tin mà BKHost mang đến.

Lựa chọn phiên bản quản lý mà bạn muốn cài đặt.

+ Install ISA Server services : giúp máy tính của bạn sẽ trở thành 1 trong những máy chủ cùng chạy ISA (là máy chủ, chạy trực tiếp)

+ Install Configuration Storage server : máy tính của bạn sẽ lưu trữ cấu hình được sử dụng bởi ISA Server và sử dụng nó để khôi phục kết nối khi cần thiết. (không phải là máy chủ, chạy gián tiếp)

+ Install both ISA Server services anh Configuration Storage server: là lựa chọn cài đặt cả 2 cái trên.

+ Install ISA Server Management : máy tính của bạn sẽ được sử dụng để quản lý ISA Server từ xa.

+ Sau đó hệ thống sẽ hiển thị lại các tính năng sắp được cài đặt cho máy của bạn. Chọn Next

Bước 4: Chọn “Create a new ISA Server enterprise, rồi ấn Next

+ Next thêm một lần nữa rồi chọn Add. Tiếp đến là Add Range, bạn nhập địa chỉ IP bắt đầu và địa chỉ IP kết thúc. Chọn OK, rồi chịu khó nhấn Next 3 lần tiếp theo là xong.

### 2.7.4 Cơ chế hoạt động của ISA Server

- ISA Server hoạt động như một tường lửa( Firewall)

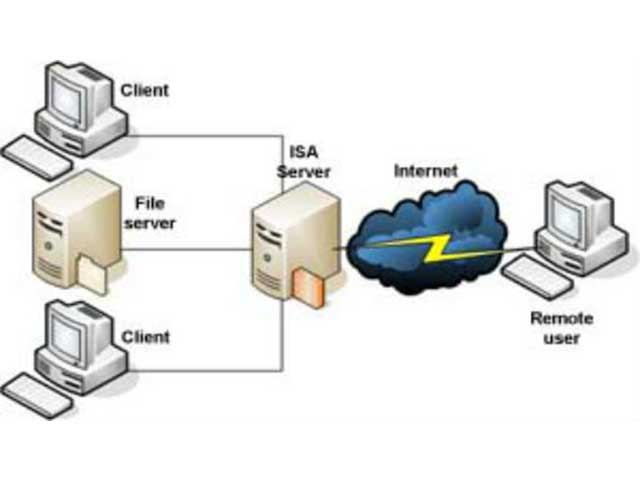
- Firewall là 1 thiết bị được đặt giữa một phân đoạn mạng với một phân đoạn mạng khác trong một mạng. Firewall được cấu hình với những ‘rule’ lọc ‘traffic’, trong đó định nghĩa những loại ‘network traffic’ sẽ được phép đi qua. Firewall có thể được bố trí và cấu hình để bào vệ mạng của tổ chức, hoặc được bố trí bên trong bảo vệ một vùng đặc biệt trong mạng.

- Trong hầu hết trường hợp, firewall được triển khai ờ vành đai mạng. Chức năng chính của firewall trong trường hợp này là đảm bảo không có ‘traffic’ nào từ internet có thể tới được ‘internal network’ của tổ chức trừ khi nó được cho phép. Ví dụ, trong tổ chức bạn có một ‘internal web Server’ cần cho ‘internet user’ có thể tới được. Firewall có thể được cấu hình để cho phép các ‘traffic’ từ Internet chỉ được truy cập đến Webserver đó.

- Về mặt chức nănh ISA Server chính là 1 firewall. Bởi mặt định, khi triển khai ISA Server, nó sẽ khóa tất cả ‘traffic’ giữa các mạng mà nó làm Server, bao gồm’ internal network’, vùng DMZ và Internet. ISA server 2006 dùng 3 loại quy tắc lọc để ngăn chặn hoặc cho phép ‘network traffic’, đó là: packet filtering,stateful filtering và application-layer filtering.

2.7.5. Cách thức hoạt động của ISA Server

- ISA Server được thiết kế bảo vệ vành đai của tổ chức mạng. Trong hầu hết trường hợp, vành đai này là giữa mạng cục bộ(LAN) của tổ chức và mạng dùng chung ( như Internet)



Hình 2.7: Mô hinh ISA đơn giản

- Mạng bên trong ( Internal network) hay gọi là mạng được bảo vệ thường được đặt trong tổ chức và có sự giám sát của nhân viên IT trong tổ chức. Internal network coi như đã được bảo mật một cách tương đối, tức là thông thường những User đã được chứng thực mới có quyền truy cập vật lý đến Internal network. Ngoải ra, nhân viên IT có thể quyết định những loại traffic nào được cho phép trên Internal Network.

- Thậm chí cho đủ Internal network an toàn hơn Internet, thì chúng ta cũng không nên có ý nghĩa sai lầm rằng, bạn chỉ cần bảo vệ vành đai mạng. Để bào vệ mạng của bạn 1 cách đầy đủ, bạn phải vạch ra kế hoạch bảo vệ theo chiều sâu, nó bao gồm nhiều bước để đảm bảo cho mạng của bạn được an toàn, thậm chí trong trường hợp vành đai bị ‘thủng’. Nhiều cuộc tấn công mạng gần đây như Virus và worm đã tàn phá những mạng có vành đai an toàn. ISA Server là thiết yếu trong việc bảo vệ vành đai mạng.

- Một tổ chức không có sự giám sát xem ai truy cập Internet bảo mật các traffic của mạng trên Internet. Thì bất kỳ 1 người nào trên thế giới với một kết nối Internet đều có thể xác định và truy cập vào các kết nối Internet khác sử dụng hầu như bất kỳ giao thức và ứng dụng gì.

- Ngoài ra những gói tin trên mạng gữi qua Internet không được an toàn, bởi vì chúng có thể bị bắt lấy và xem trộm bởi bất kỳ ai đang chạy Packet Sniffer trên 1 phân đoạn mạng Internet. Packet Sniffer là 1 ứng dụng mà bạn có thể sử dụng để bắt lấy và xem tất cả các traffic trên 1 mạng, điều kiện để bắt được traffic mạng là Packet Sniffer phải kết nối được đến phân đoạn mạng giữa 2 router.

- Internet là 1 phát minh khó tin và đầy quyến rũ. Bạn có thể tim kiếm trên mạng này nhiều thông tin hữu ích. Bạn có thể gặp gỡ những người khác,chia sẻ với họ sỡ thích của bạn và giao tiếp với họ. Nhưng đồng thời, Internet cũng là 1 nơi nguy hiểm, rất đơn giản, bởi lẻ ai cũng truy cập được.

- ISA có thể đem lại sự an toàn cho vành đai:

+ Cho phép truy cập nặc danh đến website dùng chung ( public website), trong khi đó lọc ra mã độc hại nhằm đến việc gây hại website.

+Chứng thực User từ tổ chức của đối tác trước khi gán quyền truy cập đến Website dùng riêng( private website).

+ Cho phép truy cập VPN giữa những vùng địa lý khác nhau, nhờ đó mà User ở chi nhánh văn phòng có thể truy cập đến tài nguyên trong Internal Network.

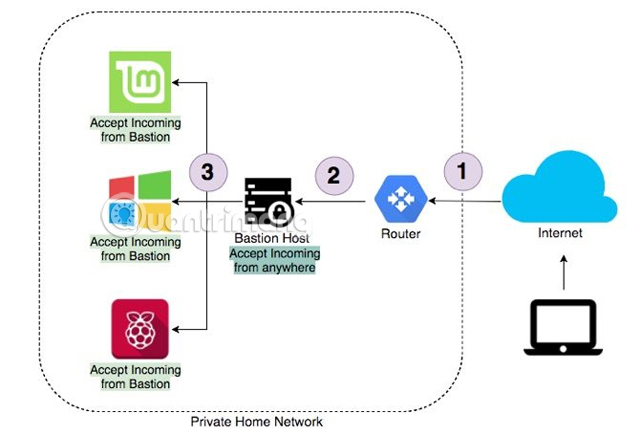
+ Cho phép nhân viên ở xa truy cập Internal Mail Server,và cho phép Client truy cập VPN đến Internal File Server,

- Áp đặc chính sách truy cập Internet của tố chức hòng giới hạn những giao thức được dùng tới ‘user’ và lọc từng ‘request’ để chắc chắn họ chỉ đang truy cập đến các tài nguyên Internet cho phép.

### 2.7.6 Các mô hình triển khai của ISA Server

**-** ISAServer 2006 có thể chạy với nhiều mô hình. Nếu chạy với tính năng Firewall ISA Server sẽ có 2 Interface hoăc nhiều Interface. Một số mô hình có thể kể đến khi sử dụng ISA Server 2006 là Bastion Host, Backend Firewall, và Proxy Server only( chỉ sữ dụng ISA Server 2006 làm Proxy Server, không tận dụng được khả năng Firewall của sàn phẩm này.

**\* Mô hình Bastion-Host:**



Hình 2.8: Mô hình Bastion-Host

- Mô hình mạng Bastion Host với Firewall ISA Server( có thể là Application hoặc Appliance đều được)

- Trong mô hình này, ISA Server một mình bảo vệ cho hệ thống mạng LAN và cung cấp Internet cho User trong mạng LAN. Trong mạng LAN của ISA Server co thể có Domain Controller, DHCP Server, DSN Server, Web Server, Mail Server. Những Server này có thể sử dụng trong mạng LAN, hoặc được sử dụng trực tiếp từ Internet User ( chỉ đối với Web Server và Mail Server đôi khi Domain controller cũng được sử dụng để chứng thực cho Internet User). Trong hệ thống LAN của ISA lúc này bao gồm 2 hệ thống LAN ( 1 là Internal cho User trong công ty và 1 là hệ thống DMZ chứa các Server được truy cập trực tiếp từ Internet User).

**\* Mô hình Back-End Firewall:**

**-** Mô hình thứ 2 này cũng thường được sử dụng. ISA Server nhẹ gánh hơn các mô hình khác là bảo vệ mạng LAN trong trường hợp FrontEnd Firewall bị đánh sập, các Server vùng mạng DMZ bị tấn công và từ đó Hackers có thể tấn công tiếp vào trong mạng LAN.

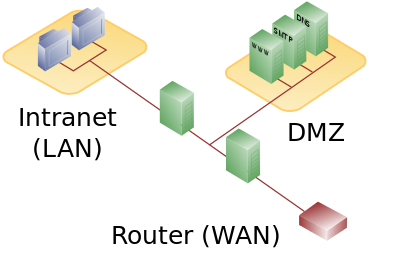
- ISA Server đóng vai trò Back-End Server cho 1 Firewall khác. Khu vực giữa Frontend và Backend Firewall là vùng DMZ chứa các Server sẽ được Published cho Internet Users.

- ISA Server có thể làm FronEnd Firewall, nhưng trong Version từ 2004 trở đi, Microsoft khuyến cáo nên dùng ISA Server( dạng Appliciton) với vai trò BackEnd là tốt nhất. Appliance Performance tốt hơn và bảo mật hơn( vì nhẹ hơn hệ điều hành).

- Trong mô hình này, ISA Server cũng mạng 2 Interface, kết nối đến hệ thống LAN có DMZ và Gateway của ISA Server sẽ là Internal của FrontEnd Firewall. Cấu hình trên Firewall và Router nói chung, nên sử dụng Routing Table đề cấu hình cho các thiết bị này. Với ISA Server, Routing Table được cấu hình bằng dịch vụ Routing and Remote Access hoặc Route ADD Command.

**\* Mô hình Three-homed:**

**-** ISA Server có trách nhiệm nặng nhất là bảo vệ mạng LAN, đống thời bảo vệ mạng DMZ chứa các Server để được truy cập từ Internet User.



Hình 2.9: Mô hình Three-home

- Mô hình Three-homed với ISA Server làm Firewall, DMZ và LAN đều kết nối vào ISA Server, mỗi mạng kết nối với ISA Server bằng một Interface riêng với Network ID khác nhau. ISA Server đóng vai trò, Router và Firewall cho các mạng này.

- ISA Server sẽ có 3 Interface kết nối với 3 Network khác nhau: Extranal, Internal và DMZ kết nối với DMZ Network. Mô hình này giống với Bastion Host, chỉ có thêm 1 Interface DMZ để tách mạng DMZ ra khỏi mạng LAN. Mạng DMZ tách biệt khỏi mạng LAN để không bị tấn công từ phía DMZ thường xuyên được truy cập từ Internet nên nguy cơ tấn công rất cao. Microsoft xem DMZ Network như Semi-Trusted Network.

### 2.7.7. ISA Server bảo mật truy cập Internet

**-** Hầuhết các tổ chức đều phải cho nhân viên cua mình truy cập Internet và sử dụng World Wide Web như 1 nguồn tài nguyên và 1 công cụ giao tiếp. Điều đó có nghĩa là không tổ chức nào tránh được việc sử dụng Internet, và việc bảo mật kết nối Internet trở nên thiết yếu.

- ISA Server có thể dùng bảo mật các kết nối của máy trạm đều đến nguồn tài nguyên internet. Để làm được điều đó, bạn phải cấu hình tất cả các máy trạm đều phải thông qua ISA Server để kết nối Internet. Khi bân cấu hình như vậy, ISA Serversẽ hoạt động như 1’proxy server’ giữa máy trạm trong mạng tổ chức và nguồn tài nguyên trên Internet.

- Điều này có nghĩa là khi một máy trạm gởi yêu cầu đến Web Server trên internet, thì sẽ không có kết nối trưc tiếp giữa máy trạm đó là Web Server. Thành phần ‘proxy server’ trên ISA Server sẽ làm việc trưc tiếp với Web Server( thay máy trạm gởi yêu cầu đến Web Server, cũng như thay Web Server hồi đáp lại cho máy trạm trong mạng cục bộ).

- Nhờ đó mà thông tin trên mạng của máy trạm sẽ không bị phơi bày ra mạng bên ngoài. Và việc máy trạm dùng ứng dụng gì để truy cập Internet hoặc truy cập đến tài nguyên gì trên Internet cũng được ISA Server kiểm soát. ISA Server cũng hoạt động như một’ catching server’.

## 2.8. ISA Client là gì?

- Phần mềm tường lửa máy khách (Firewall client) là một phần mềm được cài đặt trên các hệ điều hành Windows nhằm cung cấp sự bảo mật và khả năng truy cập nâng cao.

### 2.8.1. Triển khải Firewall Client

**-** Firewall Client được cài đặt ở các máy Client, có chế độ xác thực và tự động dò tìm ISA Server với cơ chế Auto Discovery trên ISA. Phiên làm việc giữa Client cà ISA Server thông qua port mặc định: 80, vì vậy ta cần tạo Access Rule cho phép Internal Network truy xuất qua lại với Local Host Network thông qua giao thức HTTP:

+ Rule Name: Allow Access Internal & Local Host

+ Action: Allow

+ Protocols: Internal, Local Host

+ Destination: Internal, Local Host

+ User Sets: All User.

### 2.8.2. Firewall Client làm việc như thế nào

- Firewall client giải quyết vấn đề bằng sử dụng các địa chỉ được định nghĩa bởi ISA Firewall Network trên máy khách hiện có. ISA Firewall Network cho các Firewall client cụ thể có tất cả địa chỉ có thể từ giao diện mạng được kết nối đến ISA Firewall Network của chính Firewall client. Tình huống này tạo nên một thú vị trong ISA firewall, nhiều gia đình có nhiều ISA Firewall Network được kết hợp với các adapter mạng khác. Nhìn chung, tất cả các host được đặt bên trong cùng một adapter mạng (không quan tâm đến ID mạng) được xem xét như là một phần của cùng ISA Firewall Network và tất cả sự truyền thông giữa các host trên ISA Firewall Network phải được qua Firewall client.

- Các địa chỉ cho ISA Firewall Network được định nghĩa trong suốt quá trình cài đặt của phần mềm ISA firewall, nhưng bạn có thể tạo các mạng khác sau khi cài đặt được hoàn tất. Điển hình, sau khi cài đặt, chỉ có ISA Firewall Network bên trong được tạo cho bạn và bạn cần phải tạo một cách thủ công ISA Firewall Network khác nếu có nhiều hơn 2 NIC trên ISA Firewall của bạn.

### 2.8.3. Ứng dụng của ISA Client

• Cho phép thẩm định dựa trên nhóm người dùng hoặc một người dùng riêng lẻ cho tất cả các ứng dụng Winsock bằng sử dụng các giao thức TCP và UDP.

• Cho phép người dùng và thông tin ứng dụng được ghi lại trong file bản ghi của tường lửa ISA.

• Cung cấp hỗ trợ nâng cao cho các ứng dụng mạng gồm giao thức phức hợp có yêu cầu đến kết nối thứ cấp.

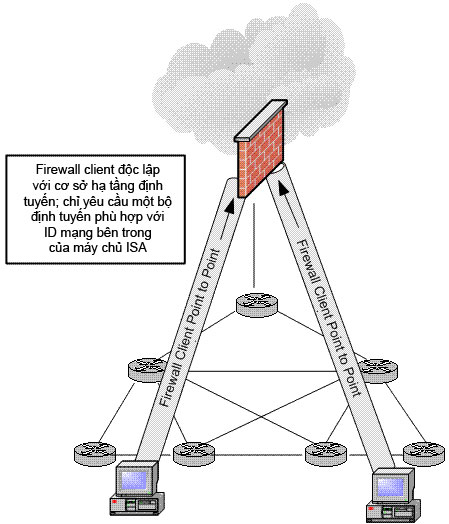
• Cung cấp hỗ trợ “proxy” DNS cho tường lửa máy tính.

• Cho phép bạn đưa ra các máy chủ yêu cầu giao thức phức hợp mà không cần sự hỗ trợ của bộ lọc ứng dụng.

• Cơ sở hạ tầng định tuyến mạng là trong suốt đối với tường lửa máy khách.

• Cho phép thẩm định dựa trên nhóm người dùng hoặc người dùng riêng biệt đối với các ứng dụng Winsock bằng sử dụng giao thức TCP và UDP.

- Phần mềm Firewall client gửi thông tin người dùng một cách trong suốt đến tường lửa ISA. Điều này cho phép bạn tạo các nguyên tắc truy cập để áp dụng cho nhóm hay người dùng riêng lẻ, hạn chế hay cho phép truy cập vào giao thức, trang, hoặc nội dung dựa vào tài khoản người dùng hoặc hội viên nhóm. Kiểm soát truy cập đi ra của các nhóm hoặc người dùng riêng lẻ là rất quan trọng. Không phải tất cả người dùng đều yêu cầu các mức truy cập như nhau và người dùng chỉ nên được phép truy cập vào giao thức, trang và nội dung mà họ yêu cầu để thực hiện công việc của họ.



Hình 2.10: Các kết nối Firewall client vào ISA 2004

### 2.8.4. Ưu điểm và Ý nghĩa của Firewall client

|  |  |
| --- | --- |
| Ưu điểm của Firewall client | Ý nghĩa |
| Thẩm định tốt dựa trên người dùng hay các nhóm đối với giao thức Winsock TCP và UDP | Thẩm định tốt dựa trên người dùng hay nhóm đối với các ứng dụng bằng sử dụng TCP và UDP cho phép bạn kiểm soát một cách chặt chẽ truy cập đi ra và có thể thực hiện nguyên lý đặc quyền tối thiểu để bảo vệ không chỉ chính mạng của bạn và còn bảo vệ cho mạng của cả công ty khác. |
| Tên người dùng và thông tin ứng dụng được lưu trong bản ghi của ISA 2004 firewall | Các kiểm soát truy cập nhóm và người dùng mạnh đã làm tăng sự bảo mật cho firewall đối với mạng của bạn thì tên người dùng và thông tin tên ứng dụng được lưu trong các bản ghi của ISA 2004 firewall lại làm tăng trách nhiệm giải trình và cho phép bạn dễ dàng nghiên cứu các trang, giao thức và ứng dụng nào mà người dùng đang chạy phần mềm Firewall client được truy cập. |
| Hỗ trợ nâng cao cho các ứng dụng và giao thức mạng | Firewall client có thể truy cập ảo vào bất kỳ giao thức dựa trên TCP và UDP nào, thậm chí những thành phần sử dụng các giao thức phức hợp cần đến nhiều kết nối chính và thứ cấp. Trái lại, SecureNAT client lại cần đến một bộ lọc ứng dụng trên the ISA 2004 firewall để hỗ trợ cho các giao thức phức hợp. Xét tổng thể Firewall client giảm được TCO so với giải pháp ISA 2004 FW. |
| Proxy DNS hỗ trợ cho Firewall client | ISA 2004 firewall có thể xử lý tên nhân danh các Firewall client. Điều này đã loại bỏ được trách nhiệm xử lý Internet host name đối với máy tính Firewall client và cho phép ISA 2004 firewall giữ sự lưu trữ DNS về các yêu cầu xử lý tên gần đây. Tính năng DNS proxy này cũng nâng cao cấu hình bảo mật cho Firewall client bởi vì nó đã loại trừ yêu cầu Firewall client được cấu hình để sử dụng một máy chủ DNS công để xử lý Internet host name. |
| Cho phép công bố các máy chủ yêu cầu giao thức mạng phức hợp | Các nguyên tắc Web và Server Publishing hỗ trợ giao thức đơn giản, ngoài ra có một ứng dụng được cài đặt trên ISA 2004 firewall như bộ lọc ứng ụng FTP Access. Bạn có thể cài đặt phần mềm Firewall client trên một máy chủ công cộng để hỗ trợ các giao thức phức hợp có thể được yêu cầu nếu bạn muốn chạy một máy chủ trò chơi trên mạng. Trong thời gian tới Microsoft cũng chính thức hỗ trợ cấu hình này và họ nhắc nhở rằng bạn cần phải có một chương trình C++ để hỗ trợ ứng dụng của bạn. |
| Cơ sở hạ tầng định tuyến mạng hoàn toàn trong suốt đối với firewall client | Không giống như SecureNAT client, dựa vào cơ sở hạ tầng định tuyến của tổ chức để sử dụng ISA 2004 firewall như tường lửa truy cập Internet, Firewall client chỉ cần biết định tuyến cho địa chỉ IP trên giao diện bên trong của ISA 2004 firewall. Điều này làm giảm được vấn đề quản lý yêu cầu để hỗ trợ cho Firewall client so với SecureNAT client. |

### 2.8.5. Cảnh báo bảo mật ISA FIREWALL

- Có nhiều giao diện trên cùng một ISA firewall. Tuy nhiên, chỉ có mạng đơn mới có thể có tên Internal (bên trong). Mạng bên trong có một nhóm các máy tính có độ tin cậy tuyệt đối (ít nhất cũng đủ tin tưởng không yêu cầu đến tường lửa mạng đối với các việc truyền thông giữa chúng). Bạn cũng có thể có nhiều mạng bên trong, nhưng các mạng bên trong bổ sung thêm này có thể được đặt trong dãy địa chỉ bên trong của mạng bên trong khác. Xem xét một cách tỉ mỉ ISA Firewall System Policy sau khi cài đặt được hoàn tất để hạn chế sự truyền thông giữa ISA Firewall và Internal Network mặc định chỉ cho truyền thông được yêu cầu cho kịch bản của bạn.

- Mặc dù vậy, cấu hình tập trung của Firewall client có thể được thực hiện trên ISA Firewall Network; vì vậy bạn có thể kiểm soát được các thiết lập Firewall client tên mỗi mạng cơ bản. Điều này cho phép bạn có được phép đo về sự kiểm tra các thiết lập cấu hình Firewall client được quản lý trên mỗi mạng như thế nào. Mặc dù giải pháp này không giúp đỡ trong kịch bản mạng trong mạng, nơi có nhiều ID mạng được đặt đằng sau cùng một card giao diện mạng.

- Trong kịch bản mạng trong mạng, bạn có thể sử dụng file locallat.txt LAT nội bộ để ghi đè các thiết lập mạng bên trong tập trung nếu thấy nó là cần thiết. Nhìn chung, kịch bản mạng trong mạng không tạo ra nhiều vấn đề đáng kể cho Firewall client. Sự cải thiện đáng kể nhất mà ISA 2004/6 Firewall client có được hơn so với các phiên bản trước (Winsock Proxy Client 2.0 và ISA Server 2000 Firewall Client) là bạn có tùy chọn để sử dụng một kênh được mã hóa giữa the Firewall client và ISA firewall.

- Nhớ rằng, Firewall client gửi các ủy nhiệm người dùng trong suốt đến ISA firewall. ISA Firewall client mã hóa kênh để giữ bí mật. Lưu ý rằng bạn có thể tùy chọn việc cấu hình ISA firewall cho phép truyền thông kênh kiểm soát không bảo mật và bảo đảm bảo mật.

### 2.8.6. Một số cách phòng chống tấn công

**-** Khi bạn phát hiện máy chủ mình bị tấn công hãy nhanh chóng truy tim địa chỉ IP đó và cấm không cho dữ liệu đến máy chủ.

- Dùng tính năng lọc dữ liệu của Router/firewall để loại bỏ các packet không mong muốn, giảm lượng lưu thông trên mạng và tải của máy chủ.

- Sữ dụng các tính năng cho phép đặt rate limit trên router/ firewall để hạn chế số lượng packet vào hệ thống.

- Nếu bị tấn công do lỗi của phần mêm hay thiết bị thì nhanh chóng cập nhật các bản sữa lỗi cho hệ thống đó hoặc thay thế.

- Dủng một số cơ chế, công cụ, phần mềm để chống lại TCP SYN Flooding.

- Tất cả các dịch vụ khác nếu có trên máy chủ để giảm tải và có thể đáp ứng tốt hơn. Nếu được có thể nâng cấp các thiết bị phần cứng để nâng cao khả năng đáp ứng của hệ thống hay sử dụng thêm các máy chủ cùng tính năng khác để phân chia tài.

- Tạm thời chuyển máy chủ sang một địa chỉ khác.

### 2.8.7. Khả năng kết nối VPN

- Cung cấp Wizard cho phép cấu hình tự động sitetosite VPN ở 2 văn phòng riêng biệt. tất nhiên ai thích cấu hình bằng tay tại từng điểm một cũng được. tích hợp hoàn toàn Quanratine.

- Stateful filtering and inspection (cái này thì quen thuộc rồi), kiểm tra đầy đủ các điều kiện trên VPN Connection, Site to site, secureNAT for VPN Clients, ...

- Cho phép Public luôn 1 VPN Server khác trong Intranet ra ngoài Internet, hỗ trợ PPTP, L2TP/IPSec, IPSec Tunnel sitetosite (với các sản phẩm VPN khác)

### 2.8.8. Về khả năng quản lý

- Dễ dàng quản lý

- Rất nhiều Wizard

- Backup và Restore đơn giản.

- Cho phép ủy quyền quản trị cho các User/Group

- Log và Report chi tiết cụ thể.

- Cấu hình 1 nơi, chạy ở mọi nơi (bản ISA Enterprise)

- Khai báo thêm server vào array dễ dàng (không khó khăn như hồi ISA 2000, 2004 )

- Tích hợp với giải pháp quản lý của Microsoft: MOM

- SDK.

### 2.8.9. Nhiệm vụ bảo mật SSL.

Xác thực server: Cho phép người sử dụng xác thực được server muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hoá công khai để chắc chắn rằng certificate và public ID của server là có giá trị và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của client. Điều này rất quan trọng đối với người dùng. Ví dụ: khi gửi mã số credit card qua mạng thì người dùng thực sự muốn kiểm tra liệu server sẽ nhận thông tin này có đúng là server mà họ định gửi đến không.

Xác thực Client: Cho phép phía server xác thực được người sử dụng muốn kết nối. Phía server cũng sử dụng các kỹ thuật mã hoá công khai để kiểm tra xem certificate và public ID của server có giá trị hay không và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy của server không. Điều này rất quan trọng đối với các nhà cung cấp. Ví dụ như khi một ngân hàng định gửi các thông tin tài chính mang tính bảo mật tới khách hàng thì họ rất muốn kiểm tra định danh của người nhận.

Mã hoá kết nối: Tất cả các thông tin trao đổi giữa client và server được mã hoá trên đường truyền nhằm nâng cao khả năng bảo mật. Điều này rất quan trọng đối với cả hai bên khi có các giao dịch mang tính riêng tư. Ngoài ra, tất cả các dữ liệu được gửi đi trên một kết nối SSL đã được mã hoá còn được bảo vệ nhờ cơ chế tự động phát hiện các xáo trộn, thay đổi trong dữ liệu. (đó là các thuật toán băm – hash algorithm).

**2.8.10. Tại sao nên sử dụng SSL**

Khi bạn đăng ký tên miền để sử dụng các dịch vụ website, email v.v… luôn có những lỗ hổng bảo mật cho hacker tấn công, SSL bảo vệ website và khách hàng của bạn.

An toàn dữ liệu: dữ liệu không bị thay đổi bởi hacker.

Bảo mật dữ liệu: dữ liệu được mã hóa và chỉ người nhận đích thực mới có thể giải mã.

Chống chối bỏ: đối tượng thực hiện gửi dữ liệu không thể phủ nhận dữ liệu của mình.

Tiêu chuẩn xác thực – SSL chỉ được cung cấp bởi các đơn vị cấp phát chứng thư (CA) có uy tín trên toàn thế giới sau khi đã thực hiện xác minh thông tin về chủ thể đăng ký rất kỹ càng mang lại mức độ tin cậy cao cho người dùng Internet và tạo nên giá trị cho các website, doanh nghiệp cung cấp dịch vụ.

# KẾT QUẢ THỰC NGHIỆM

3.1. Kịch bản thực nghiệm

Ta sẽ sử dụng ISA Server 2006 để set-up một số Rule trong máy Server.

3.2. Yêu cầu thực nghiệm

Chuẩn bị sẵn 2 máy ảo : 1 DC, 1 Server.

Cấu hình sẵn địa chỉ Ip cho cả 2 máy

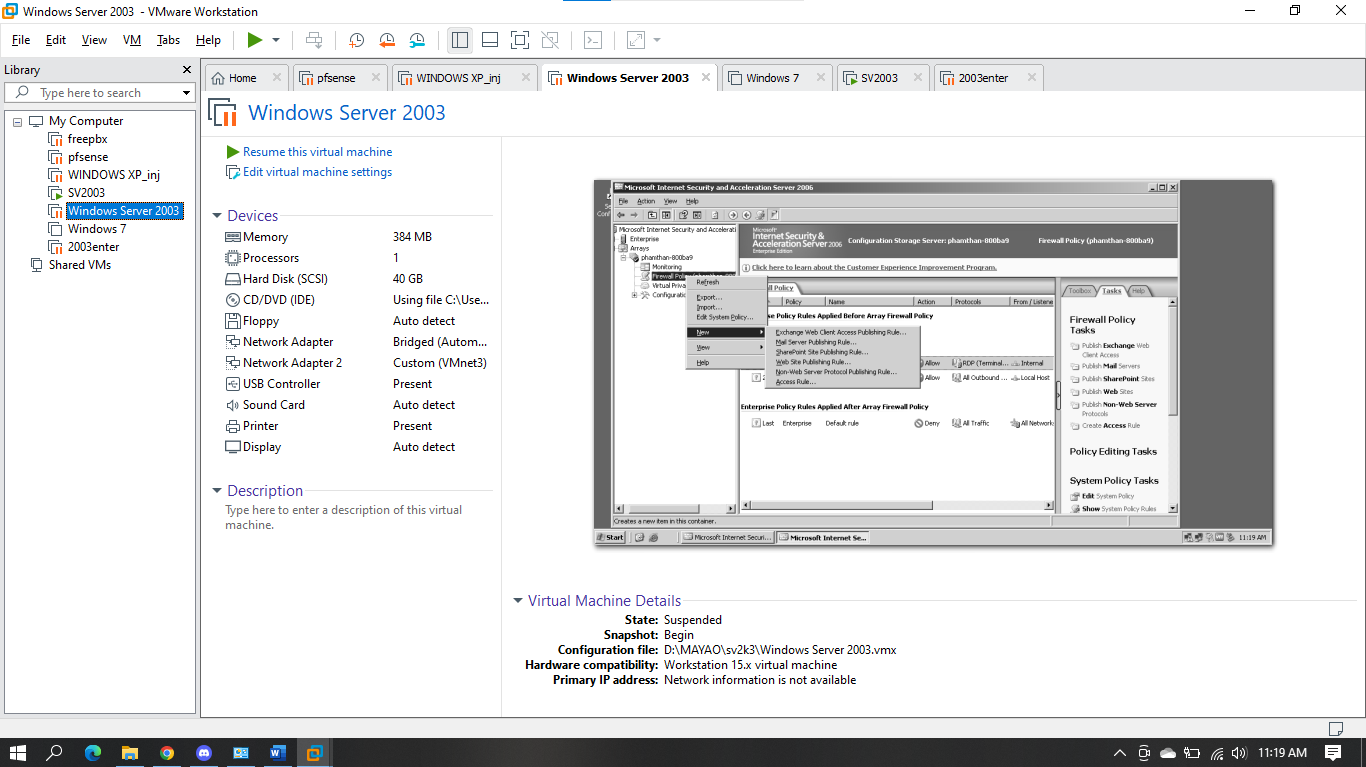
Nâng cấp Domain Controller, Web Server cho máy DC

3.3. Công cụ sử dụng

Máy ảo VMWare Workstation.

Một server firewall ISA chạy trên hệ điều hành microsoff.

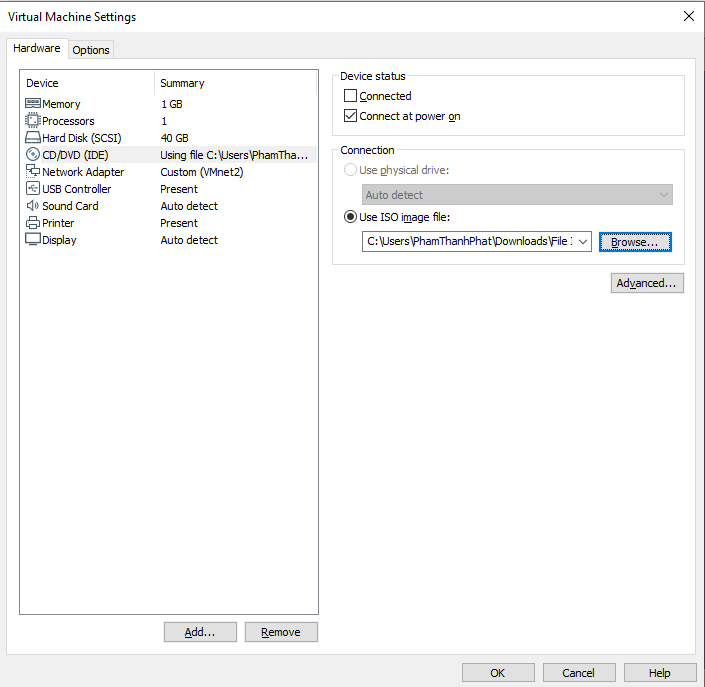
Một mấy windows server.



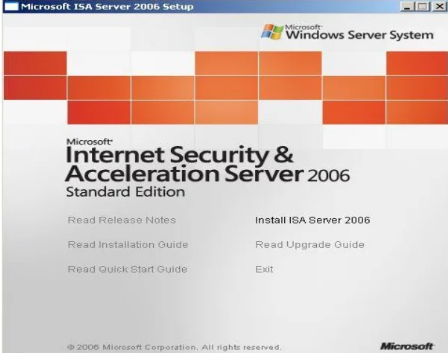
Hình 3.1: Máy ảo VMWare Workstation

## 3.4. Các bước thực hiện

### 3.4.1. Cài đặt ISA Server 2006



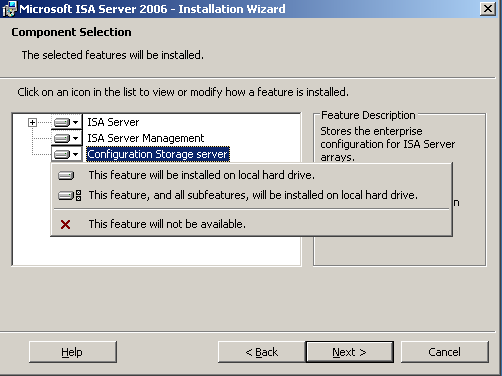
Chúng ta vào setting chọn CD/DVD để add file iso của firewall ISA vào



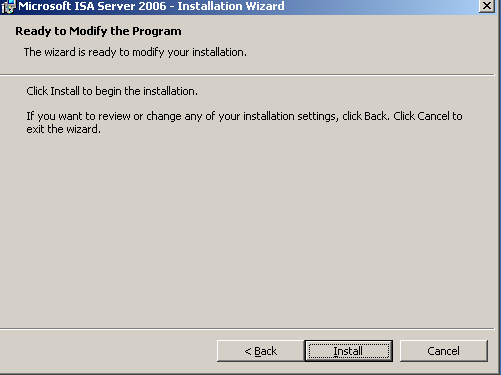
Chạy file iso lên chúng ta được giao diện cài đặt -> chọn install ISA server 2006



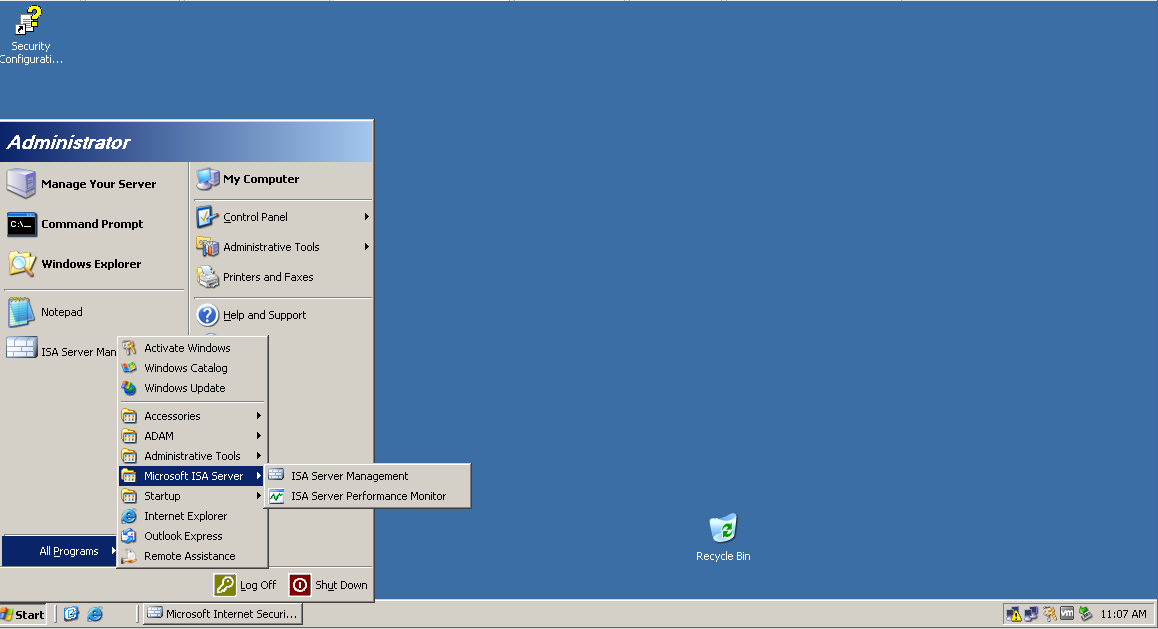
Tiếp tục chọn Next



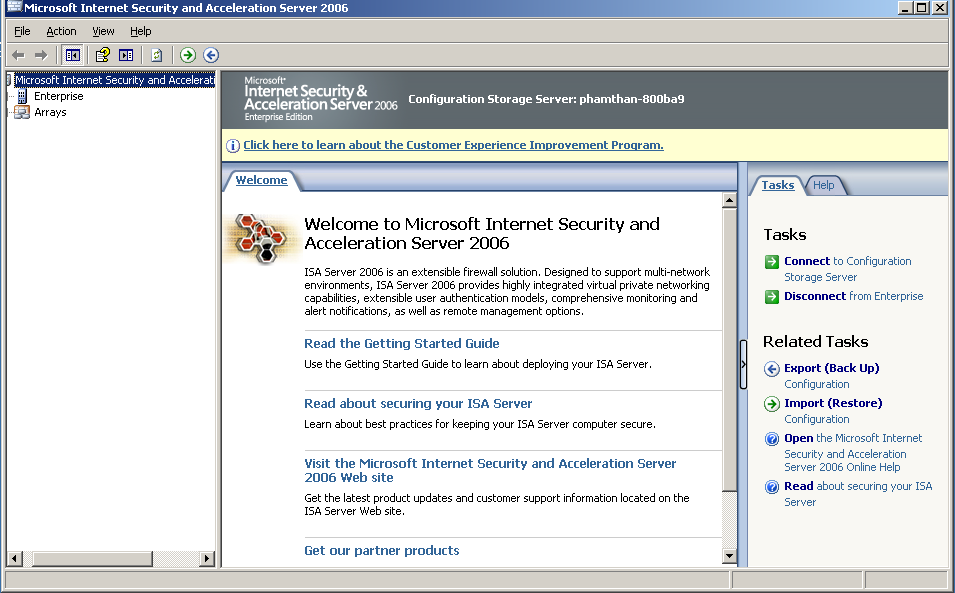
Chọn this feature will be installed on local hảd drive-> Next



Chọn install chờ firewall ISA cài đặt.



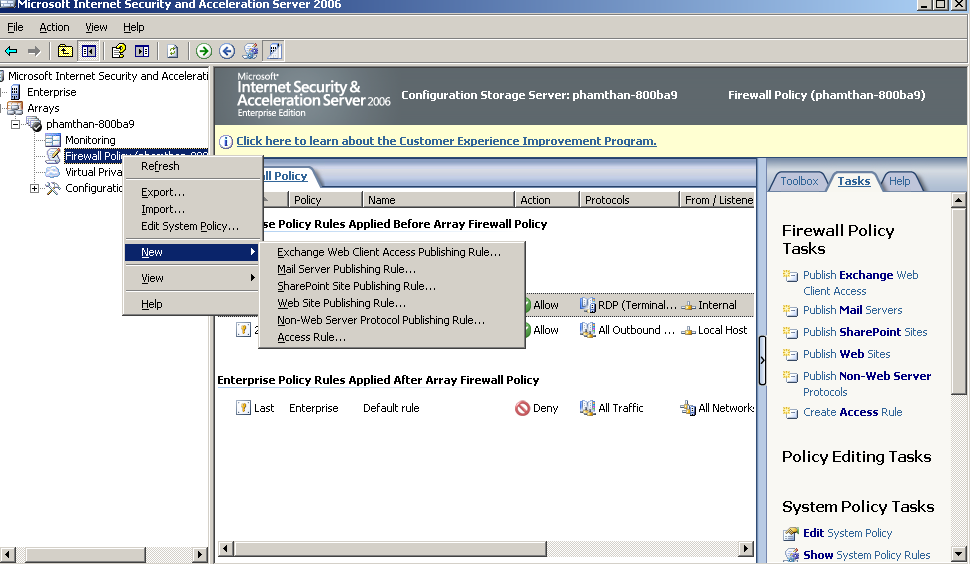
Khi cài đặt xong chúng ra mở cửa sổ windows lên và chọn All program chọn Microsoft ISA Server để mở ISA



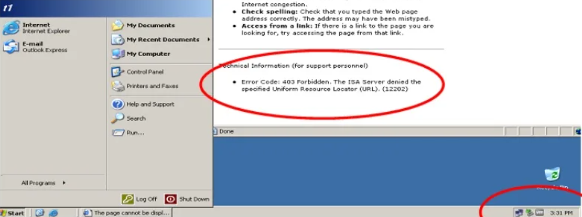
Đây là giao diện khi chúng ta chạy firewall IS

### 3.4.2. Cấu hình Access Rule trên máy ISA

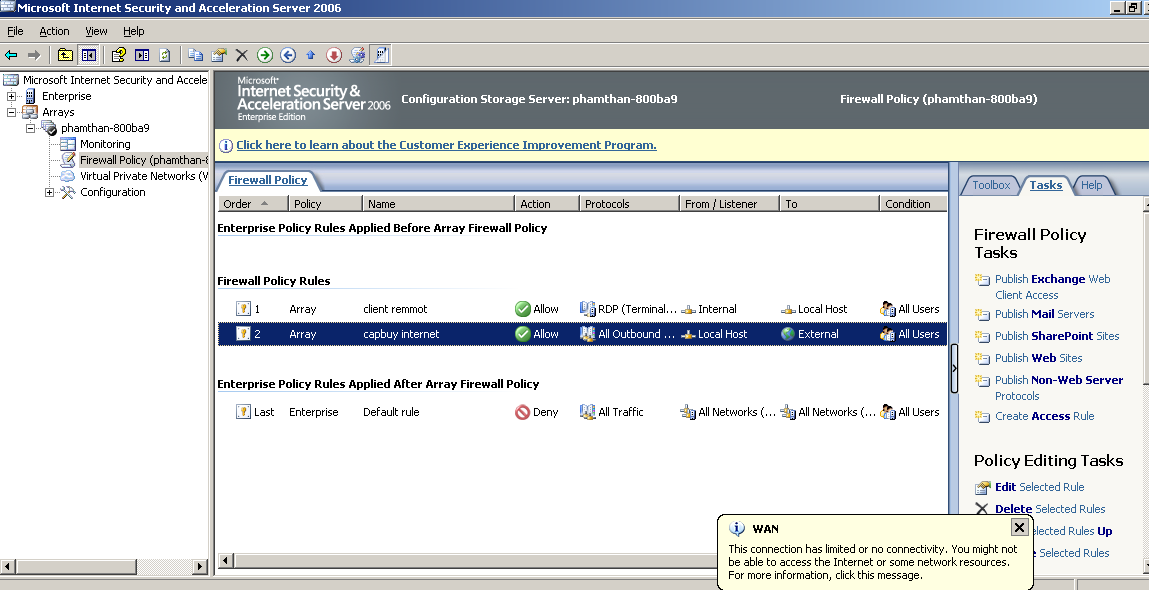
Chúng ta sẽ chọn firewall Policy -> chọn new -> Access rule để cấu hình rule



Hình 3.2: Cấu hình Access Rule trên máy ISA



Hình 3.3: Cấu hình những trang Web được và không được truy cập



Hình 3.4: Cấu hình Access Rule cho phép máy ISA truy cập mạng

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## 4.1. Kết luận

Nắm được phương pháp xây dựng một hệ thống bảo mật

Nắm được các kiến thức và vận dụng về tường lửa FireWall ISA, Firewall client, Firewall server.

Hiểu và biết cách ứng dụng vào nhằm ngăn chặn việc truy cập dữ liệu trái phép, bảo vệ nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống.

Thông qua thời gian học tập và tìm hiểu về giao thức Firewall ISA dưới sự hướng dẫn của thầy, chúng em bước đầu đã xây dựng được một hệ thống bảo mật. Hệ thống này đã đạt được các yêu cầu về tiêu chuẩn để ngăn chặn việc truy cập dữ liệu trái phép, bảo vệ nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Hệ thống đạt được sự an toàn, chất lượng cao, chi phí phù hợp, giảm thiểu được khá nhiều khả năng rủi ro bị đánh cắp thay đổi, nâng cao chất lượng của hoạt động thương mại.

## 4.2. Hướng phát triển

Tìm hiểu được các tính năng bảo bảo vệ nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống.

Tiếp tục tìm hiểu và phát triển các chức năng cao hơn.

Thu thập được nhiều kiển thức hơn trong quá trình tạo ra hệ thống bảo mật

Lắng nghe ý kiến người dùng để được hoàn thiện hơn

# TÀI LIỆU KHAM KHẢO

<https://quantrimang.com/tim-hieu-ve-isa-firewall-client-phan-1-37791>

<https://quantrimang.com/cai-dat-va-cau-hinh-isa-server-firewall-2004-chuong-1-19678>

<https://tailieu.vn/doc/tim-hieu-ve-isa-firewall-client-87817.html>

<https://www.tailieudaihoc.com/doc/206708.html>

<https://www.youtube.com/watch?v=v7TELlSIFns>

<https://bkhost.vn/blog/isa-server-la-gi/>

<https://www.tailieudaihoc.com/doc/172639.html>