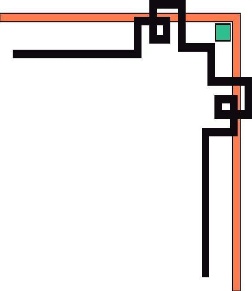
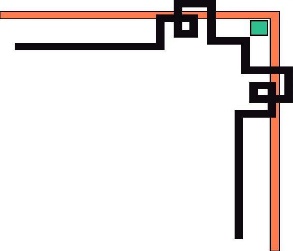
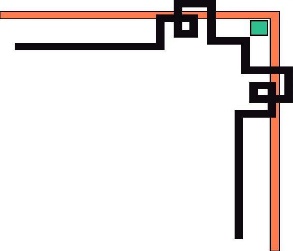
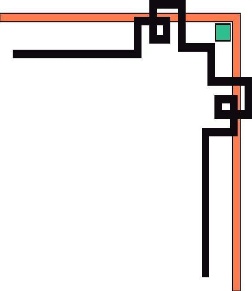
**TRƯỜNG ĐH CÔNG NGHIỆP TP. HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**



# LỜI CẢM ƠN

**Đồ án học phần 3**



Tphcm,ngày 17 tháng 05 năm 2015

**Sinh viên thực hiện :**

**Nguyễn Mạnh Cường :11250631**

**Trần Nguyễn Lộc:11230851**

**GVHD :ThS.Nguyễn Minh Hải**

**ĐỀ TÀI: XÂY DỰNG FIREWALL TMG 2010 TRONG BẢO MẬT MẠNG DOANH NGHIỆP**

**LỜI CẢM ƠN**

-Chúng em xin chân thành cảm ơn quí thầy cô đã giúp đỡ chúng em thực hiện đề tài này. Đặc biệt thầy Nguyễn Minh Hải đã tận tình giúp đỡ, chỉ bảo chúng em. Trong quá trình làm đề tài có gặp nhiều khó khăn cũng nhờ thầy động viên, giúp đỡ .

- Chúng em xin trân trọng cảm ơn những tình cảm quí báu mà các thầy cô Trường Đại Học Công Nghiệp Tp.HCM đã truyền đạt cho chúng em, những kinh nghiệm, kỹ thuật trong quá trình học tập cũng như cách thức xây dựng đề tài này.

-Tuy nhiên, do thời gian có hạn nên chúng em không thể phát huy hết những ý tưởng. Trong quá trình làm đề tài, không thể tránh khỏi những sai xót, mong nhận được sự đóng góp và cảm thông của quí thầy cô.

# NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

Tphcm,ngày..... tháng …... năm ......

Giáo viên hướng dẫn

Kí tên

# NHẬN XÉT CỦA GIÁO VIÊN PHẢN BIỆN

Tphcm,ngày...... tháng ...... năm .....

Giáo viên phản biện

Kí tên

MỤC LỤC

[CHƯƠNG I. GIỚI THIỆU TỔNG QUAN VỀ FOREFRONT THREAT MANAGEMENT GATEWAY 2010 2](#_Toc419570286)

[**1.GIỚI THIỆU VỀ FIREWALL** 2](#_Toc419570287)

[1.1 Khái niệm 2](#_Toc419570288)

[1.2 Cách thức hoạt động 2](#_Toc419570289)

[1.2.1 Packet filtering 2](#_Toc419570290)

[1.2.2 Application gateway 3](#_Toc419570291)

[1.2.3 Circuit level gate 4](#_Toc419570292)

[1.3 Hạn chế 5](#_Toc419570293)

[**2.CÁC YÊU CẦU THỰC TẾ TRONG DOANH NGHIỆP** 6](#_Toc419570294)

[**3.GIỚI THIỆU VỀ THREAT MANAGEMENT GATEWAY 2010** 6](#_Toc419570295)

[3.1 Sự ra đời 6](#_Toc419570296)

[3.2 Các phiên bản 7](#_Toc419570297)

[**4.CÁC TÁC ĐỘNG ẢNH HƯỞNG ĐẾN SỰ ỔN ĐỊNH VÀ HIỆU SUẤT CỦA TMG 2010** 9](#_Toc419570298)

[4.1 Cấu hình phần cứng 9](#_Toc419570299)

[4.2 Các dịchvụ cơ sở hạ tầng](#_Toc419570300) 10

[4.3 Kết nối mạng](#_Toc419570301) 10

[CHƯƠNG II.CHỨC NĂNG CỦA THREAT MANAGEMENT GATEWAY 2010](#_Toc419570302) 11

[**1.FIREWALL** 12](#_Toc419570303)

[1.1 Enhance NAT 12](#_Toc419570304)

[1.2 Voice over IP 12](#_Toc419570305)

[1.3 Access rule 12](#_Toc419570306)

[**2.SECURE WEB GATEWAY** 13](#_Toc419570307)

[2.1 URL filtering 13](#_Toc419570308)

[2.2 HTTP filtering 15](#_Toc419570309)

[2.3 HTTPS inspection 16](#_Toc419570310)

[2.4 Malware inspection 16](#_Toc419570311)

[**3.REMOTE ACCESS GATEWAY** 18](#_Toc419570312)

[**4.E-MAIL PROTECTION** 19](#_Toc419570313)

[**5.INTRUSION PREVENTION** 20](#_Toc419570314)

[5.1 Monitoring 20](#_Toc419570315)

[5.2 Instrusion prevention system 20](#_Toc419570316)

[5.3 Network inspection system 21](#_Toc419570317)

[**6.CÁC PHƯƠNG PHÁP TẤN CÔNG VÀ PHÒNG CHỐNG TRONG TMG 2010** 21](#_Toc419570318)

[6.1. HTTP Request 21](#_Toc419570319)

[6.2. UDP Flood 25](#_Toc419570320)

[6.3. TCP SYN Flood 28](#_Toc419570321)

[6.4. IP half-scan 33](#_Toc419570322)

[CHƯƠNG III.DEMO 35](#_Toc419570323)

[**1.CHỨC NĂNG PHÁT HIỆN VÀ PHÒNG CHỐNG TẤN CÔNG TRONG TMG 2010** 35](#_Toc419570324)

[**2. CÁC CUỘC TẤN CÔNG TỪ BÊN NGOÀI** 36](#_Toc419570325)

[2.1.HTTP Request 36](#_Toc419570326)

[2.2.UDP Flood 38](#_Toc419570327)

[2.3.TCP SYN Flood 39](#_Toc419570328)

[2.4.IP Half-scan 40](#_Toc419570329)

[CHƯƠNG IV. TỔNG KẾT 42](#_Toc419570330)

[1.KẾT LUẬN 42](#_Toc419570331)

[2.HƯỚNG PHÁT TRIỂN 42](#_Toc419570332)

[TÀI LIỆU THAM KHẢO 43](#_Toc419570333)

# LỜI MỞ ĐẦU

-Những năm trở lại đây, đất nước chúng ta đang trong quá trình hội nhập và phát triển , song song quá trình đó là sự phát triển vượt bậc của tất cả các ngành, trong đó phải kể tới ngành công nghệ thông tin-một trong những ngành mũi nhọn của nước nhà Việt Nam của chúng ta.

-Cùng với nhu cầu phát triển của ngành công nghệ thông tin thì vấn đề bảo mật cũng đang là một trong vấn đề mà tất cả các nước phải đối phó , trong đó có cả Việt Nam.Các thiết bị bảo mật hệ thống mạng phần cứng và phần mềm nổi tiếng lần lượt ra đời như Cisco-thiết bị phần cứng mạng của Microsoft………., Snort thiết bị phần mềm.

-Trước sự tấn công không ngừng , cùng với cách thức tấn công nguy hiểm của tin tặc thì việc lựa chọn một tường lửa thích hợp cho mỗi doanh nghiệp là điều vô cùng quan trọng, nó quyết định đến sự sinh tồn của mỗi công ty .Và đề tài ứng dụng bảo mật hệ thống mạng trong doanh nghiệp cũng chính là đề tài mà nhóm em nghiên cứu-Xây dựng Firewall TMG 2010 Trong Bảo Mật Mạng Doanh Nghiệp

-Với đề tài này,chúng em sẽ làm rõ được các chức năng quan trọng của TMG 2010 trong các doanh nghiệp, đặc biệt là chức năng cảnh báo và phòng chống được các đợt tấn công từ bên ngoài, từ đó có thể giúp doanh nghiệp lựa chọn , so sánh với các phần mềm firewall khác phù hợp với nhu cầu sử dụng của mình giúp việc bảo mật của hệ thống mạng công ty được bảo mật một cách tốt nhất.

# CHƯƠNG I. GIỚI THIỆU TỔNG QUAN VỀ FOREFRONT THREAT MANAGEMENT GATEWAY 2010

## 1.GIỚI THIỆU VỀ FIREWALL

### 1.1 Khái niệm

-Tường lửa là thiết bị phần cứng hoặc phần mềm có nhiệm vụ lọc, kiểm soát dữ liệu từ bên trong ra bên ngoài hệ thống và ngược lại qua các rule đã được cài đặt trước đó.Mục đích của việc sử dụng tường lửa là giúp tạo ra vùng kết kết nối an toàn từ bên trong ra bên ngoài hệ thống cũng như ngăn chặn việc truy cập trái phép dữ liệu từ bên ngoài vào bên trong hệ thống, ngăn chặn việc rò rỉ phát tán thông tin ra bên ngoài , đồng thời nó là công cụ hữu ích cho việc quản lý, phân quyền truy cập cho nhân viên được tốt hơn.

**1.2 Cách thức hoạt động**

Một firewall bao gồm một hoặc nhiều thành phần sau đây:

* Packet Filtering.
* Application Gateway.
* Circuit Level Gate.

**1.2.1 Packet filtering**

-Bộ lọc gói tin là thành phần quyết định số phận của gói tin mà nó nhận được. Nó sẽ kiểm tra gói tin mà nó nhận được coi có thỏa mãn một trong các số các qui tắc hay không. Các qui tắc này dựa trên các thông tin ở phần header của gói tin bao gồm các thông tin sau:

* IP Source Address ( Địa chỉ IP nguồn).
* IP Destination Address ( Địa chỉ IP đích).
* Protocol (TCP, UDP, ICMP, IP tunnel).
* TCP/UDP source port (Cổng TCP/UDP nguồn).
* TCP/UDP destination port(Cổng TCP/UDP đích).
* ICMP message type (Dạng thông báo ICMP).

-Nếu gói tin thỏa mãn các qui tắc lọc gói thì nósẽ được đi qua firewall, nếu không gói tin sẽ bị bỏ đi. Do đó firewall có thể ngăn cản các kết nối vào các máy chủ hoặc mạng nào đó, hoặc cấm truy cập vào mạng nội bộ từ những địa chỉ bị cấm.

* Ưu điểm:

+ Có sẵn trong router nên chi phí thấp.

+ Tự thực hiện lọc , không yêu cầu người dùng thao tác gì cả.

* Nhược điểm:

+ Việc thiết lập bộ lọc khá là phức tạp, đòi hỏi người quản trị cần có hiểu biết nhất định về gói tin

+ Không thể đọc được nội dung của gói tin nên vẫn có thể gây hại cho máy người dùng.

**1.2.2 Application gateway**

Cổng ứng dụng hoạt động bằng cách thức gọi là Proxy Server. Nó được dùng để:

- Che dấu các client bên trong mạng sau một IP duy nhất.

- Lọc các URL và kiểm tra nội dung của gói tin.

- Ngoài ra , thành phần này của firewall cũng tiến hành lưu bản copy của các Web trên Server nhằm giảm sự lặp lại các truy vấn vào cùng 1 trang web. Khi 1 client bên trong mạng muốn truy cập vào trang Web trên Internet thì proxy nhận truy vấn từ host, sau đó nó sẽ tìm trang web đó trong bộ nhớ đệm. Nếu có thì proxy sẽ gửi trang Web về cho host. Nếu không có thì proxy sẽ chuyển yêu cầu này đến đích thay cho host.

-  Ngoài ra , Proxy chỉ làm việc cho 1 ứng dụng cụ thể được chỉ định bởi người quản trị mạng.

* Ưu điểm:

+Người quản trị có thể kiểm soát từng dịch vụ trong mạng bởi vì người quản trị có toàn quyền quyết định máy chủ nào có thể truy cập các dịch vụ.

+ Việc lưu lại các thông tin truy cập giúp người quản trị dễ dàng kiểm soát hệ thống nếu có sự cố xảy ra.

+ Dễ dàng cấu hình và kiểm tra hơn, bởi vì mọi thứ diễn ra ở tầng Application.

* Nhược điểm :

+Phải cấu hình trên các máy người dùng để sử dụng được dịch vụ proxy.

+Người dùng không thể thiết lập proxy nếu không có kiến thức nhât định về proxy.

**1.2.3 Circuit level gateway**

-Circuit Level Gateway là một chức năng chạytrên một cổng ứng dụng cụ thể.Nhiệm vụ của cổng mạch chỉ là cho phép các kết nối TCP đi qua mà không thực hiện việc xử lý nào. Do đó nó làm cho hệ thống firewall dễ dàng sử dụng cho người dùng trong mạng nội bộ muốn trực tiếp truy câp tới các dịch vụ internet, trong khi vẫn cung cấp chức năng bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

* Ưu điểm:

+ Giúp cho việc truy cập dịch vụ internet nhanh hơn và không cần sự can thiệp của người quản trị nếu có sự cố xảy ra.

* Nhược điểm :

+ Việc bảo mật gói tin là không an toàn tuyệt đối vì nó có nhiệm vụ chuyển tiếp các kết nối TCP chứ không có nhiệm vụ kiểm tra các gói tin.

+Vì không thể kiểm tra gói tin nên có khả năng máy tính bị nhiễm malware

**1.3 Hạn chế**

**-**Một hệ thống mạng có firewall bảo vệ chưa chắc đã an toàn tuyệt đối bởi nó có những nhược điểm sau:

* Firewall không thể chống lại các cuộc tấn công không đi qua tường lửa như “ARP-Poisoning” ,….
* Firewall không thể chống lại các cuộc tấn công có nguồn gốc từ bên trong nội bộ .Ví dụ như một nhân viên cố ý hoặc vô tình hợp tác với kẻ tấn công bên ngoài, khi đó thì tường lửa sẽ trở nên vô tác dụng.
* Firewall không thể chống lại hoàn toàn các cuộc tấn công của các tập tin bị nhiễm virus vì virus thì ngày càng đa dạng ngày càng phức tạp.

### 

## 2.CÁC YÊU CẦU THỰC TẾ TRONG DOANH NGHIỆP.

-Ngày nay , việc sử dụng internet đang được sử dụng phổ biến , mỗi doanh nghiệp đều tự trang bị cho mình một đường truyền internet riêng biệt. Tuy nhiên vấn đề bảo mật trong doanh nghiệp vẫn chưa được quan tâm đúng mức. Một số hậu quả xấu vẫn có thể xảy ra đối với mỗi doanh nghiệp bất cứ lúc nào như:

-Nhân viên truy cập internet bất hợp pháp trong giờ hành chính.

-Sự rò rỉ , mất mát dữ liệu trong nội bộ công ty bởi các hacker chuyên nghiệp.

-Vi rút lây lan trong hệ thống mạng một cách nhanh chóng.

-Các phần mềm gián điệp được cài vào mà không thể phát hiện.

-Trước những vấn đề đó ,việc bảo mật dữ liệu là vô cùng quan trọng-nó quyết định đến sự sinh tồn của một công ty.Vì thế việc lựa chọn một firewall thích hợp là vấn đề doanh nghiệp đặt lên hàng đầu , và tường lửa TMG 2010 là một trong những lựa chọn thích hợp nhất cho mỗi doanh nghiệp để phòng ngừa và đối phó với những vấn đề này.

## 3.GIỚI THIỆU VỀ THREAT MANAGEMENT GATEWAY 2010

## 3.1 Sự ra đời

- MICROSOFT FOREFONT THREAT MANAGEMENT GATEWAY2010(TMG 2010) được phát hành vào ngày 17 tháng 11 năm 2009 và được xây dựng trên nền tảng của ISA Server 2006.

-TMG 2010 là loại firewall thông minh có khả năng phòng chống các phần mềm độc hại , tăng cường bảo vệ web,các dịch vụ mạng , hỗ trợ Window Server 2008 và Window Server 2008 R2, giúp bảo vệ hệ thống an toàn và bảo vệ cho truy cập mạng một cách an toàn.

- Phiên bản Service Pack 1 của sản phẩm này được phát hành vào ngày 23 tháng 6 năm 2010 bao gồm một số tính năng mới hỗ trợ Window Server 2008 R2 và SharePoint 2010.

**3.2 Các phiên bản**

-Microsoft cho ra mắt hai phiên bản TMG 2010 :

+ Forefont TMG 2010 Standard Edition

+ Forefont TMG 2010 Enterprise Edition

Mặc dù triển khai trên hai cơ sở hạ tầng mạng khác nhau , cả hai phiên bản bao gồm các tính năng giống nhau và khả năng kiểm soát truy cập . Tuy nhiên chúng vẫn khác nhau .

* ***Bảng so sánh tính năng của hai bản TMG 2010 Standard Edition và TMG 2010 Enterprise Edition***

|  |  |  |
| --- | --- | --- |
| Tính năng | Standard Edition | Enterprise Edition |
| Hỗ trợ triển khai trên | Server độc lập | Server độc lập và Server được quản lí bởi EMS |
| CPU | Hỗ trợ lên tới 4 CPU | Không giới hạn |
| Lưu trữ | Cục bộ | Hỗ trợ quản lí từ xa bởi chính sách tường lửa và cấu hình |
| Quản lí dành cho doanh nghiệp | Không | Có |
| Publishing | có | Có |
| Hỗ trợ VPN | có | Có |
| Forward proxy/cache compression | Có | Có |
| Network IPS (NIS) | Có | Có |
| Email protection | Yêu cầu đăng kí bản quyền | Yêu cầu đăng kí bản quyền |
| Web Protection | Yêu cầu đăng kí | Yêu cầu đăng kí |

* ***Bảng so sánh Forefont TMG và ISA Server 2006***

|  |  |  |
| --- | --- | --- |
| Tính năng | ISA 2006 | ForeFont TMG 2010 |
| Cài đặt | Window Server 2003 SP1/R2 32bit | Window Server 2008 SP2, R2 64 bit |
| Hỗ trợ bộ nhớ | Tối đa 4GB | Nhiều hơn 4GB |
| Network layer firewall | Có | Có |
| Application layer firewall | Có | Có |
| Internet access protection(proxy) | Có | Có |
| Web cache | Có | Có |
| Publish Server | có | Có |
| IPSec VPN | Có | Có |
| Basic OWA and SharePoint publishing | Có | Có |
| URL filtering | Không | Có |
| Web antimalware | Không | Có |
| Network inspection system(NIS) | Không | Có |
| Https inspection | Không | Có |
| E-mail antimalware, antispam | không | Có |
| Cải tiến VPN | Không | Có |
| Cải tiến log và report | Không | Có |

## 4.CÁC TÁC ĐỘNG ẢNH HƯỞNG ĐẾN SỰ ỔN ĐỊNH VÀ HIỆU SUẤT CỦA TMG 2010

**4.1 Cấu hình phần cứng**

-Để TMG hoạt động ổn định và hết công suất thì phần cứng như bộ xử lí , bộ nhớ , dung lượng ổ đĩa ,… phải được cung cấp đầy đủ và mạnh mẽ để mọi chức năng của TMG hoạt động một cách trơn tru. Việc xác định sử dụng phần cứng như thế nào thật sự rất khó khăn do phụ thuộc vào nhiều yếu tố như số lượng người dùng , các tính năng sẽ được sử dụng , băng thông bạn đang có . Do đó Microsoft đã giới thiệu phần mềm Forefront TMG Capacity Planning Tool, phần mềm này sẽ tính toán dựa trên các yếu tố kể trên và đưa ra cấu hình phần cứng theo yêu cầu.

**4.2 Các dịch vụ cơ sở hạ tầng**

-Tường lửa TMG hoạt động dựa vào các dịch vụ hạ tầng như Active Directory, DNS, … để thực hiện nhiệm vụ của nó, do đó , việc cấu hình sai các dịch vụ hạ tầng hay việc kết nối chậm tới các dịch vụ hạ tầng này đều ảnh hưởng đến hiệu suất làm việc của TMG.

**4.3 Kết nối mạng**

-TMG là một tường lửa có vai trò phân phối dữ liệu , do đó , cấu hình mạng đóng vai trò rất lớn trong hiệu suất của TMG . Ví dụ như cấu hình DNS , cấu hình tường lửa TMG sau tường lửa khác để giảm các hành động xử lí ,… đều có thể làm tăng hiệu suất làm việc của TMG.

# CHƯƠNG II.CHỨC NĂNG CỦA THREAT MANAGEMENT GATEWAY 2010

****

*Sơ đồ chức năng của TMG 2010*

## 1.FIREWALL

**1.1 Enhance NAT**

-NAT (Network Address Translate) là chức năng cho phép chuyển đổi địa chỉ IP private thành địa chỉ IP public để liên lạc được với các máy ngoài internet,ngoài tính năng NAT truyền thống one-to-one ,TMG 2010 hỗ trợ tính năng đặc biệt Enhance Nat có thể chuyển đổi nhiều địa chỉ ip private thành một ip public (many-to-one) với số port khác nhau để có thể liên lạc với các ngoài internet. Ngoài ra trong phiên bản TMG 2010 này, tính năng Enhanced NAT cho phép gửi mail theo dạng one-to-one bằng NAT , có nghĩa là ta tạo 1 kết nối từ Mail server mạng nội bộ với Mail server trên internet.

**1.2 Voice over IP**

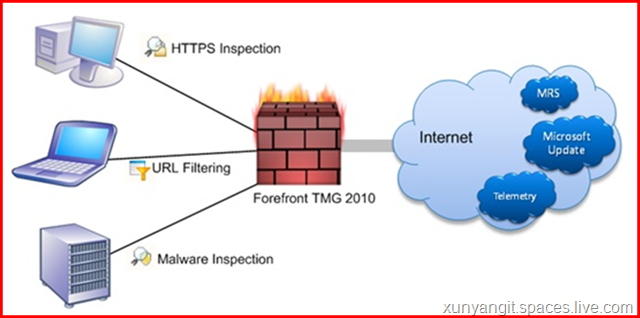
-Tính năng này cho phép kết nối và sử dụng VoIP thông qua tường lửa TMG. Voice Over IP quản lý lưu lượng sử dụng những cuộc gọi thoại hoặc video giữa các mạng nội bộ và mạng Internet.

**1.3 Access rule**

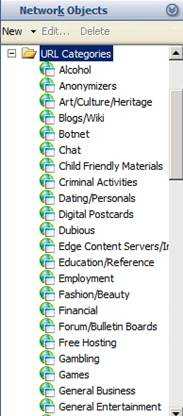
- Access Rule là tính năng được dùng để điều khiển truy cập gửi ra từ một mạng nằm sau TMG(được bảo vệ bởi tường lửa). Khi muốn một máy tính ở 1 mạng nằmsau TMG truy cập một mạng khác (gồm có Internet), bạn cần tạo một Access Rule để cho phép kết nối đó. Mặc định là không có Access Rule nào cho phép các kết nối đi qua tường lửa,do đó người quản trị phải tạo ra các rule để quản lý, phân quyền việc truy cập và sử dụng internet của Client thông qua các protocol được định sẵn.Tính năng này giúp cho việc quản lý nhân viên dễ dàng hơn đồng thời tránh được sự truy cập bất hợp pháp theo quy định của công ty.

## 2.SECURE WEB GATEWAY

Bao gồm các chức năng:

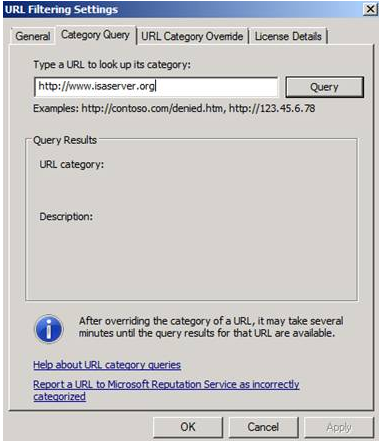


### 2.1 URL filtering

****

*Danh sách phân loại URL*

-URL (Uniform Resource Locator) là những dẫn để truy cập đến các loại tài nguyên khác nhau trong hệ thống, cho nên để ngăn truy cập đến tài nguyên nào đó trên internet thì cần dựa vào đường dẫn URL này. TMG cho phép phân loại các URL để cho người quản trị dễ dàng quản lí, người quản trị cho phép các người dùng được phép hoặc không được phép truy cập vào một trang web nào đó dựa trên các danh mục phân loại.



*Cách truy vấn URL thuộc loại danh mục phân loại nào*

-Quá trình hoạt động như sau: client gửi yêu cầu truy cập một trang web nào đó, TMG sẽ truy cập vào MRS (Microsoft reputation Service) cục bộ để biết được URL này nằm ở danh mục phân loại nào, sau đó nó tìm trong danh mục phân loại đó , nếu mà có các rule bị cấm thì nó sẽ không cho truy cập , còn nếu không bị cấm thì nó sẽ cho phép ra ngoài internet.

### [2.2 HTTP filtering](#_Toc392838933)

-HTTP Filter là một bộ lọc lớp ứng dụng, được sử dụng bởi các Web Proxy . HTTP **Filter giúp bạn giới hạn lưu lượng truy cập** bằng cách ngăn chặn theo một số tính năng như HTTP header, phương thức HTTP, nội dung của HTTP và các phần mở rộng tập tin ,…. Bằng cách lọc và chặn lưu lượng HTTP không mong muốn chúng ta có thể giới hạn số lượng lưu lượng truy cập không mong muốn thông qua TMG.

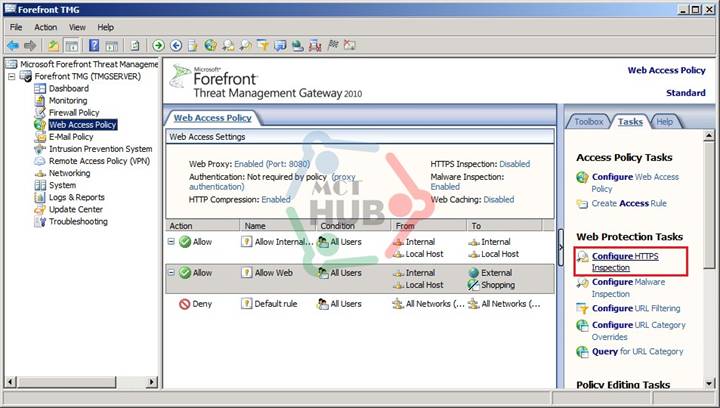


*Cấu hình HTTP Filtering*

### [2.3 HTTPS inspection](#_Toc392838934)

- HTTPS Inspection là một tính năng mới TMG , nó có thể phân tích được SSL mà trong nhiều năm đã được sử dụng như là một kẽ hở của kẻ tấn công và người sử dụng độc hại để tránh bị phát hiện.**HTTPS Inspection tăng khả năng bảo vệ người dùng của TMG Firewall, cung cấp bảo vệ người dùng khỏi các cuộc tấn công trên website.**

-Tính năng này rất quan trọng trong việc kiểm tra phần mềm độc hại và giúp bảo vệ người dùng khỏi virus download từ máy chủ e-mail trên nền web như Outlook Web Access (OWA) và các trang web HTTPS khác.



*Cấu hình HTTPS Inspection*

### 2.4 Malware inspection

**-**Chức năng này giúp phát hiện và ngăn chặn các loại mã độc được cấy vào HTTP stream, khi client vô tình truy cập vào các trang web đã được cài mã độc, lúc này mã độc sẽ đi vào hệ thống mạng và sẽ làm cho hệ thống mạng ngừng hoạt động , chính vì thế TMG hỗ trợ tính năng Malware Inspection để ngăn chặn việc này.

- Cách hoạt động của Malware Inspection:

+**Bước 1**. Client ban đầu sẽ gửi yêu cầutới máy chủ trang web và yêu cầu tải về 1 file trên đó về .

+**Bước 2**. TMG sẽ nhận yêu cầu này và kiểm tra yêu cầu này có thỏa các qui tắc nào đã đặt ra không , TMG sẽ kiểm tra nếu không thỏa hoặc yêu cầu chứa mã độc hại thì sẽ chặn yêu cầu lại.

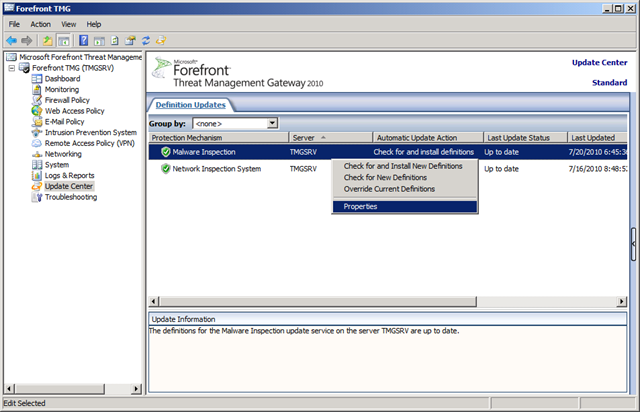
+**Bước 3**. Nếu yêu cầu hợp lệ và không chứa mã độc, TMG gửi yêu cầu đến web server để yêu cầu tải dữ liệu về .

+**Bước 4.** Web Server nhận được yêu cầu và gửi lại dữ liệu tương ứng yêu cầu của người dùng.

+**Bước 5**.TMG nhận được dữ liệu từ Web server và xử lý dữ liệu đó thông qua proxy engine.

+**Bước 6**.Nếu qui tắc có kích hoạt kiểm tra mã độc hại trong dữ liệu, thì proxy engine sẽ gửi body của dữ liệu đó đến bộ lọc mã độc hại (Malware Inspection Filter). Malware Inspection Filter sẽ tiến hành kiểm tra 64KB đầu tiên của dữ liệu, nội dung đoạn mã đó được lưu và xử lý tại bộ nhớ (RAM) mà không cần lưu vào đĩa cứng rồi mới kiểm tra mã độc hại , nhằm giảm thiểu việc tiêu tốn tài nguyên trong máy . Sau đó trao trả lại quyền kiểm soát cho proxy engine.

+**Bước 7**. Nếu dữ liệu đó không tồn tại mã độc hại, TMG gửi dữ liệu gốc lại cho người dùng. Nếu dữ liệu có mã độc hại và TMG không thể xóa mã độc hại đó, TMG sẽ gửi một trang HTML nhằm cảnh báo người dùng rằng dữ liệu này đã bị chặn tải về do có chứa mã độc hại.



*Cấu hình Malware Inspection*

## [3.REMOTE ACCESS GATEWAY](#_Toc392838936)

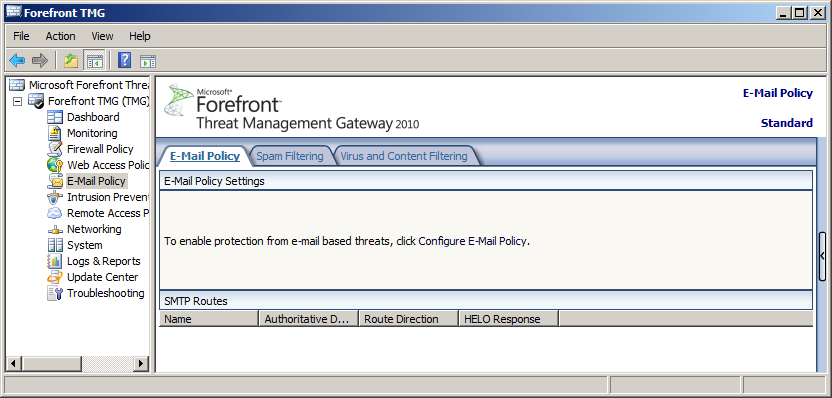
-Trong ISA 2006 , VPN chỉ cho phép client kết nối qua 2 giao **thức PPTP** và **L2TP/IPSEC** hoạt động tương đối hiệu quả. Thế nhưng nó lại có một số nhược điểm vô cùng quan trọng đó là việc chứng thực từ một nhân viên bên ngoài internet, khi nhân viên kết nối tới VPN mà môi trường mạng chỉ các port 80. 443 thì không có cách nào chứng thực VPN qua ISA.

-Để khắc phục hiểu quả vấn đề này, ngoài các giao thức hỗ trợ trong ISA , TMG còn hỗ trợ thêm giao thức Secure Socket Tunneling Protocol (SSTP) giao thức đường hầm an toàn. SSTP là một đường hầm VPN, SSTP thực hiện điều này bằng cách sử dụng giao thức HTTPscho các kết VPN để có thể đi qua các firewall, NAT và server web proxy thường được cấu hình.Bởi vì giao thức HTTPs (TCP 443) thường được sử dụng để truy cập các website được bảo vệ như các web site thương mại,do đó HTTPs thường được mở trong các firewall và có thể đi qua các Proxy web, router NAT.

## 4.E-MAIL PROTECTION

-TMG có thể quét và lọc những email spam gửi vào hệ thống , lọc những email có nội dung cấm , hỗ trợ anti-virus tránh việc phát tán virus vào trong hệ thống. TMG cung cấp 3 chức năng để bảo vệ hệ thống Mail Server là :

* E-mail Policy.
* Spam Filtering.
* Virus and Content Filtering.



*Cấu hình Email Protection*

## 5.INTRUSION PREVENTION

## 5.1 Monitoring

- Chức năng Monitoring cho phép giám sát và theo dõi các luồng dữ liệu ra vào giữa mạng nội bộ và mạng internet. Khi phát hiện ra các bất thường thì sẽ hiện ra thông báo cho nhà quản trị mạng.

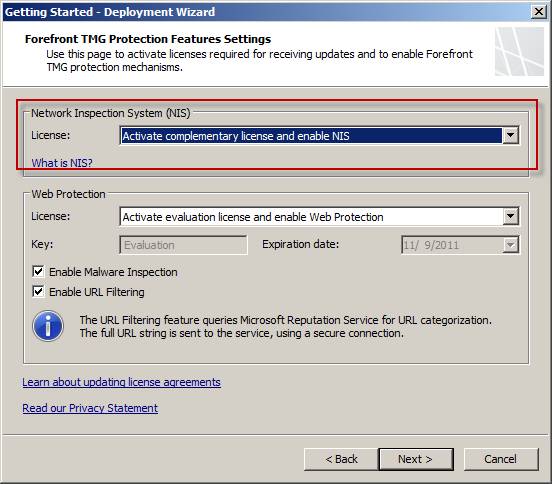
**5.2 Intrusion prevention system**

- Là “Hệ thống phòng chống xâm nhập” , có chức năng giám sát hoạt động mạng , phát hiện các nguy cơ , ngăn chặn chúng và báo cáo lại. Các phương pháp phát hiện nguy cơ được sử dụng :

* Signature-Based Detection: là phương pháp phát hiện dựa trên chữ kí , Firewall sẽ giám sát các gói tin trong mạng và so sánh với các mô hình tấn công được cấu hình và xác định trước .
* Statistical Anomaly-Based Detection: Là phương pháp phát hiện dựa trên sự bất thường của hoạt động mạng như các giao thức sử dụng, các cổng và các thiết bị kết nối .
* Stateful Protocol Analysis Detection: Stateful Protocol là việc theo dõi cũng như xử lí các gói tin đến trong quá trình truyền nhận dữ liệu. Phương pháp này hoạt động bằng cách so sánh các sự kiện của trạng thái giao thức với các qui tắc được xác định trước.

### 5.3 Network inspection system

- Network Inspection System(NIS) là hệ thống phát hiện và ngăn chặn hoàn toàn mới ,dùng để ngăn chặn việc tấn công vào hệ điều hành và các ứng dụng của Microsoft từ xa , nó được giới thiệu lần đầu tiên trong TMG 2010. NIS hoạt động dựa trên chữ kí số . Các chữ kí này được phát hành bởi Microsoft Malware Protection Center(MMPC). Khi phát hiện hệ điều hành hoặc ứng dụng có lỗ hổng thì MMPC sẽ cung cấp cho NIS 1 tập chữ kí số. NIS trong khi phân tích các gói tin , bao gồm cấu trúc gói tin và nội dung tin , nó có thể nhận dạng và khóa chặn tấn công lỗ hổng.



*Kích hoạt và cấu hình NIS*

## 6.Các phương pháp tấn công và phòng chống trong TMG 2010.

## 6.1. Http Request

-HTTP Request là một loại tấn công [DDoS](http://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html), trong đó nó sẽ khai thác các phương thức HTTP GET hoặc POST để tấn công một máy chủ web.Ta có :

**HTTP-GET Body**:

GET /demo/demo\_form.asp?name1=value1&name2=value2 HTTP/1.1

Host: www.test.com

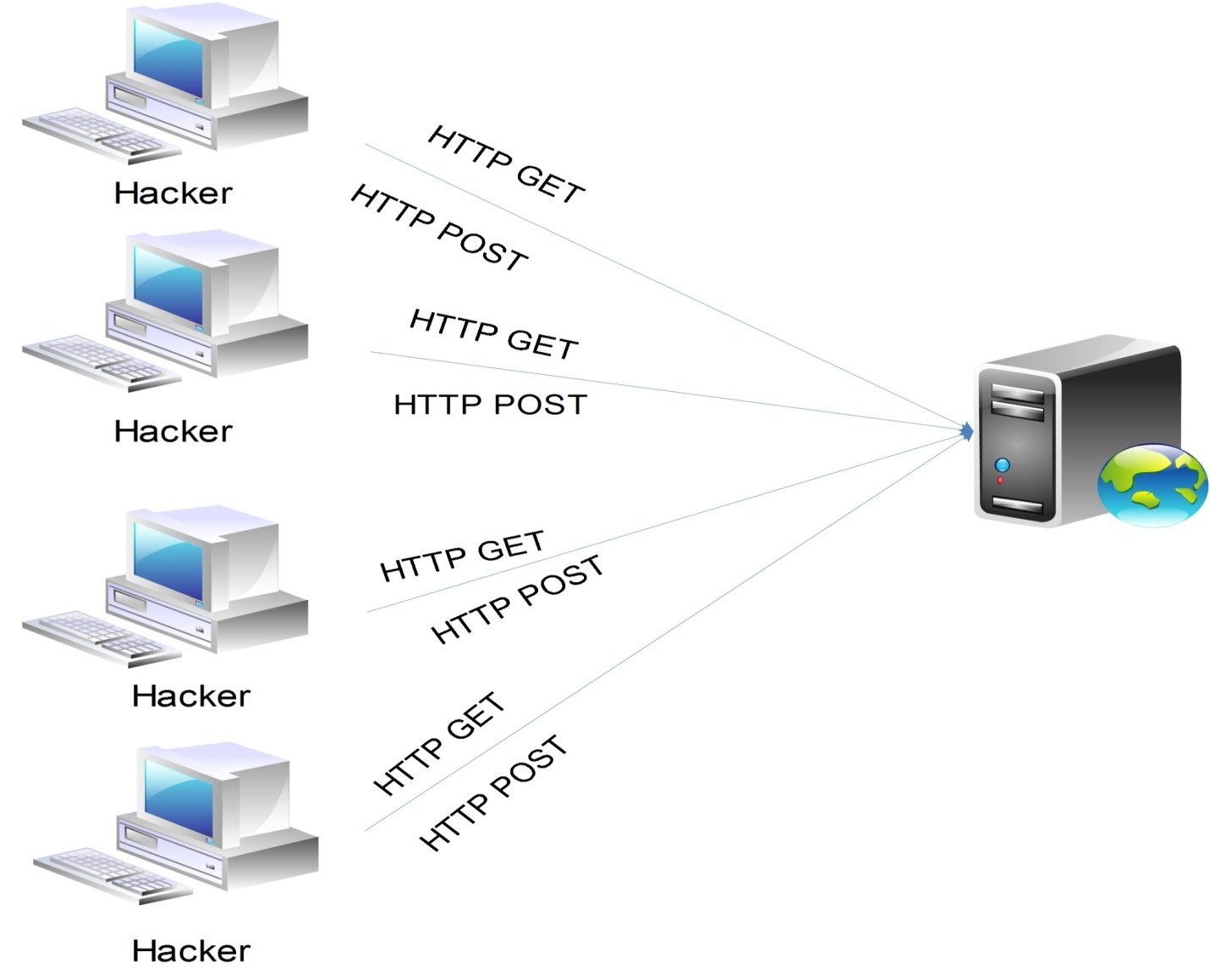
**HTTP-POST Body**:

POST /demo/demo\_form.asp HTTP/1.1

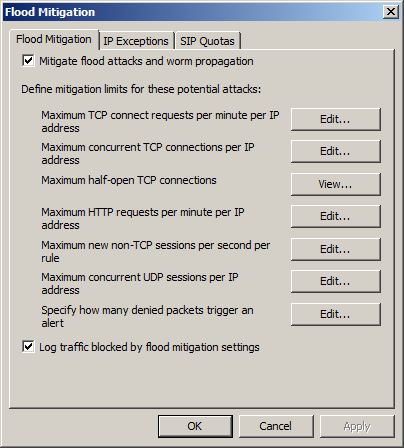
Host: www.test.com

name1=value1&name2=value2

-Khi một người dùng dùng trình duyệt web để trao đổi dữ liệu với máy chủ , nó sẽ gửi 1 trong 2 loại yêu cầu là : HTTP GET hoặc POST tới phía máy chủ . Lợi dụng việc này , người tấn công sẽ tìm mọi cách để tạo ra nhiều yêu cầu nhất có thể , để bắt máy chủ phải phân bố tài nguyên của mình để đáp ứng các yêu cầu đó.



***-Phòng chống***: Để phòng chống phương pháp tấn công ở trên , ta mở TMG lên , sau đó chọn **Intrusion Prevention System**, sau đó chọn tab **Behavioral Intrusion Detection** trong cửa sổ chính và kích **Configure Flood Mitigation Settings. Sau đó tích vào ô Mitigate flood attacks and worm propagation, ta có hình dưới đây:**

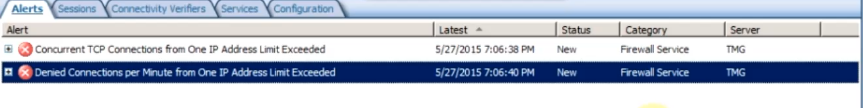


-Sau khi có bảng như trên đây , ta điều chỉnh dựa theo yếu tố dưới đây :

* Số yêu cầu HTTP tối đa trên 1 phút trên địa chỉ IP. Ta có hình sau:

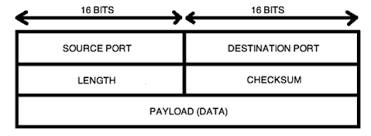


-Sau khi ta thiết lập và lưu lại thì khi 1 gói tin bất kì đi qua TMG sẽ bị chặn lại , sau đó thành phần “Packet Filtering” trong TMG sẽ tiến hành lọc gói tin theo thông số mà chúng ta vừa thiết lập , nếu gói tin thỏa mãn rule thì nó sẽ được thông qua , còn nếu gói tin của IP vi phạm thì sẽ bị chặn lại và hiện ra thông báo :



### 6.2. UDP Flood

-cấu trúc gói tin UDP :



-Quá trình tấn công UDP flood:

+Tấn công UDP flood là một kiểu tấn công từ chối dịch vụ sử dụng giao thức User Datagram Protocol(UDP) , một kiểu giao thức mạng máy tính không kết nối.

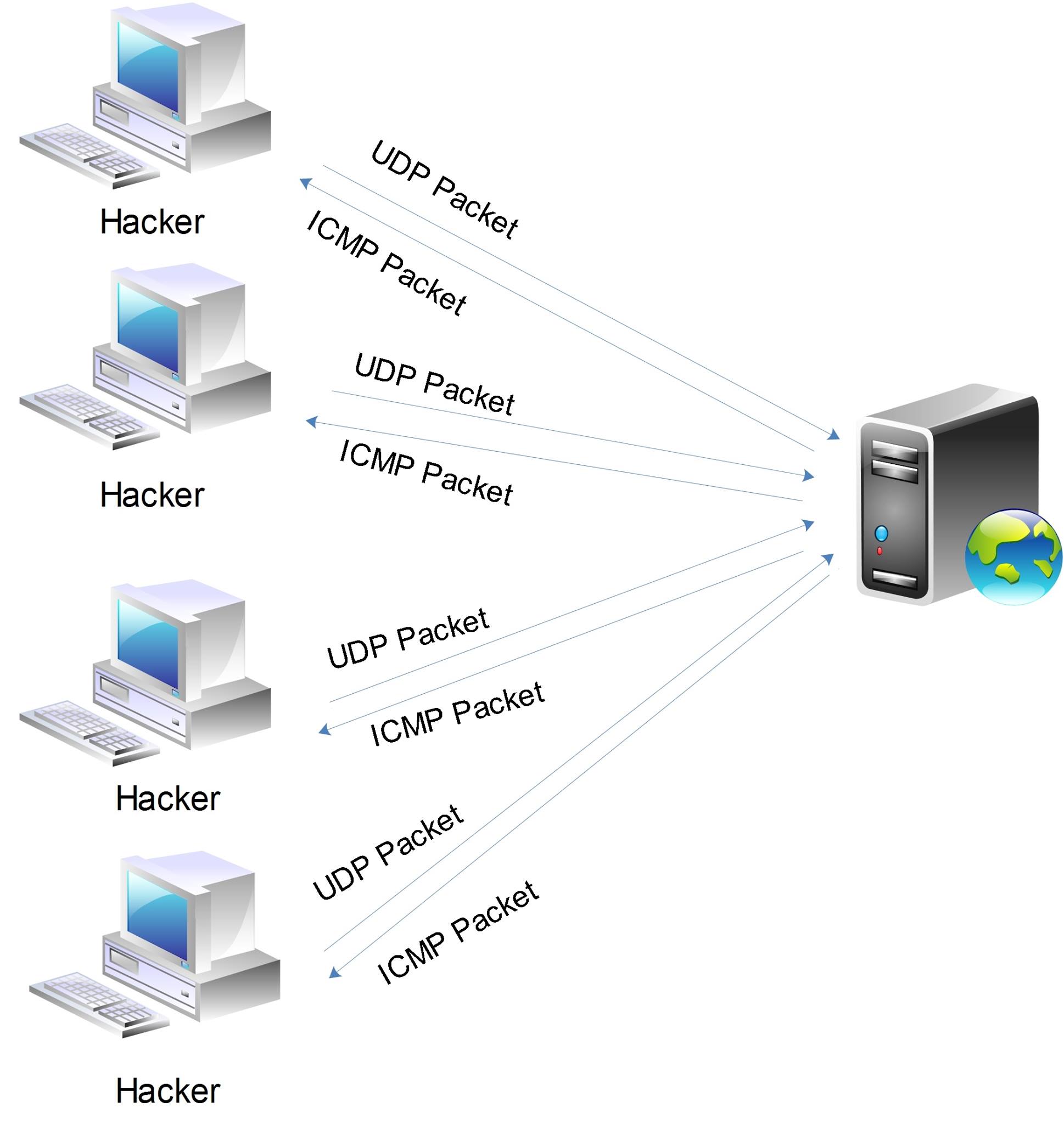
+Quá trình tấn công UDP flood có thể được bắt đầu bằng cách gửi một số lượng lớn các gói UDP đến các cổng ngẫu nhiên đến máy chủ từ xa. Kết quả là các máy dịch vụ ở xa sẽ:

-Kiểm tra các ứng dụng đang lắng nghe tại cổng

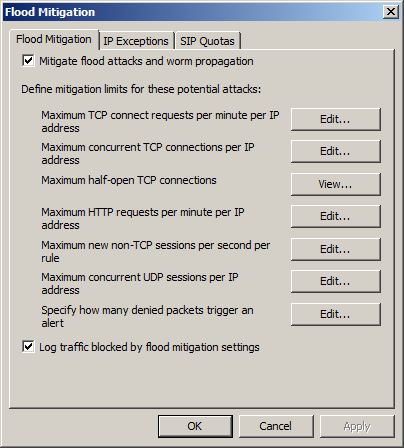
- Không thấy ứng dụng nào lắng nghe tại cổng

Kết quả là sẽ trả lời lại gói tin ICMP Destination Unreachable.

Lợi dụng điều này, kẻ tấn công sẽ gửi một số lượng lớn các gói tin UDP , hệ thống nạn nhân sẽ bị buộc gửi lại nhiều gói tin ICMP và từ đó làm khách hàng không thể truy cập được dịch vụ.



***-Phòng chống***:Để phòng chống phương pháp tấn công ở trên , ta mở TMG lên , sau đó chọn **Intrusion Prevention System**, sau đó chọn tab **Behavioral Intrusion Detection** trong cửa sổ chính và kích **Configure Flood Mitigation Settings . Sau đó tích vào ô Mitigate flood attacks and worm propagation, ta có hình dưới đây:**

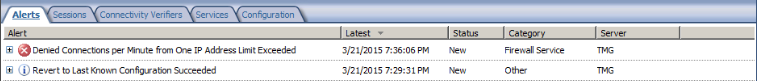


-Sau khi có bảng như trên đây , ta điều chỉnh dựa theo yếu tố dưới đây :

* Số UDP session đồng thời trên một IP tối đa. Ta có hình sau:

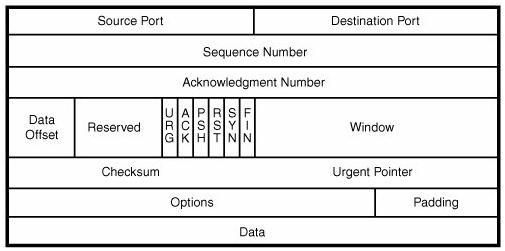


-Sau khi ta thiết lập và lưu lại thì khi 1 gói tin bất kì đi qua TMG sẽ bị chặn lại , sau đó thành phần “Packet Filtering” trong TMG sẽ tiến hành lọc gói tin theo thông số mà chúng ta vừa thiết lập , nếu gói tin thỏa mãn rule thì nó sẽ được thông qua , còn nếu gói tin của IP vi phạm thì sẽ bị chặn lại và hiện ra thông báo :



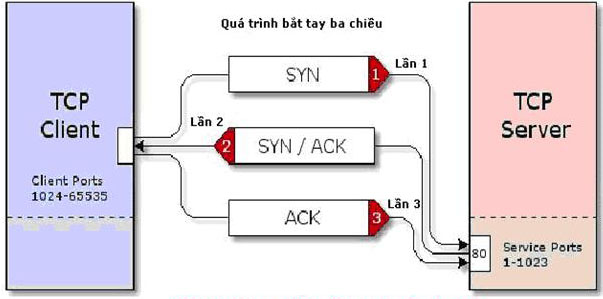
**6.3. TCP SYN Flood**

**-**Là loại tấn công DDOS bằng cách lợi dụng lỗ hổng của thủ tục kết nối TCP khi “bắt tay ba bước”. Ta có cấu trúc gói tin TCP :

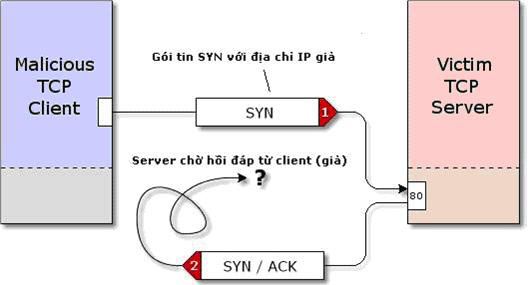


-Ta có quy trình của bắt tay 3 bước :

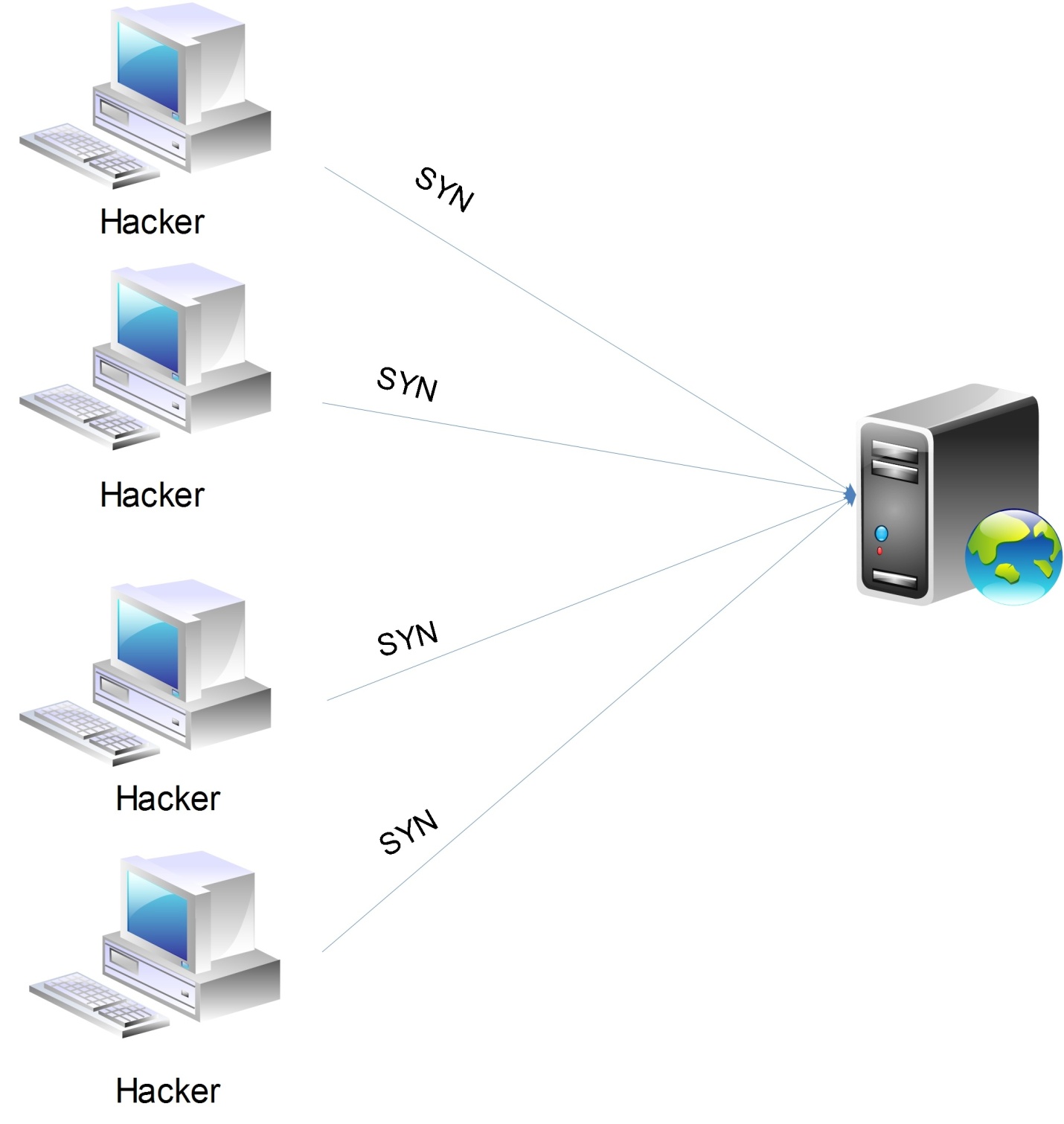
Bước 1: Máy của người dùng sẽ tiến hành gửi gói tin (gói tin chứa SYN=1) đến máy chủ để yêu cầu kết nối.   
Bước 2: Khi nhận được gói tin của máy người dùng vừa gửi, nếu máy chủ chấp nhận kết nối thì nó sẽ tiến hành gửi lại gói tin SYN/ACK nhằm thông báo cho máy người dùng biết là nó đã nhận được yêu cầu kết nối và cũng như chuẩn bị sẵn tài nguyên cho việc yêu cầu này. Server sẽ giành một phần tài nguyên hệ thống cho việc truyền , nhận dữ liệu.   
Bước 3: Cuối cùng, máy người dùng sẽ hoàn tất việc bắt tay ba bước bằng cách phản hồi lại gói tin chứa cờ ACK lại cho máy chủ và tiến hành gửi dữ liệu .



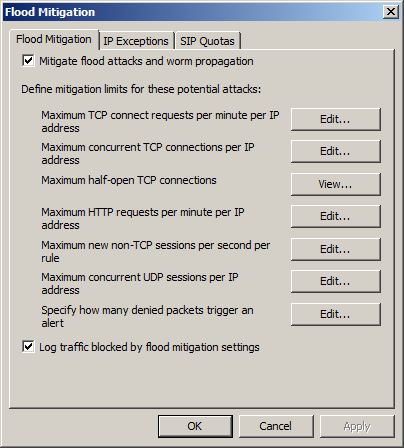
-Do TCP là 1 kết nối tin cậy nên sau khi máy chủ gửi các gói tin SYN/ACK trả lời lại máy người dùng mà không nhận lại được hồi âm để thực hiện kết nối thì nó vẫn sẽ giữ nguồn tài nguyên để chuẩn bị cho kết nối và sẽ gửi lại gói tin SYN/ACK cho máy người dùng đến khi nào nhận được hồi đáp của máy client.   
-Điều quan trọng cho việc tấn công DDOS ở đây là làm cho máy người dùng không hồi đáp lại máy chủ . Và khi có nhiều, rất nhiều máy làm như thế trong khi máy chủ vẫn lặp lại việc gửi gói tin SYN/ACK đó và đồng thời giành tài nguyên để chờ kết nối , trong khi tài nguyên của hệ thống là có giới hạn. Điều này sẽ làm cho các kết nối của người dùng hợp lệ sẽ bị chậm hoặc không kết nối được tới máy chủ.



Mô hình tấn công của **TCP SYN Flood**:



***-Phòng chống***:Để phòng chống phương pháp tấn công ở trên , ta mở TMG lên , sau đó chọn **Intrusion Prevention System**, sau đó chọn tab **Behavioral Intrusion Detection** trong cửa sổ chính và kích **Configure Flood Mitigation Settings . Sau đó tích vào ô Mitigate flood attacks and worm propagation, ta có hình dưới đây:**



Sau khi có bảng như trên đây , ta điều chỉnh dựa theo yếu tố dưới đây :

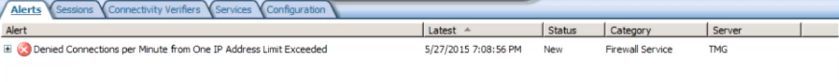
* Số yêu cầu kết nối TCP tối đa trên phút trên một IP.Ta có hình sau:



* Số kết nối TCP đồng thời tối đa trên một địa chỉ IP. Ta có hình sau:

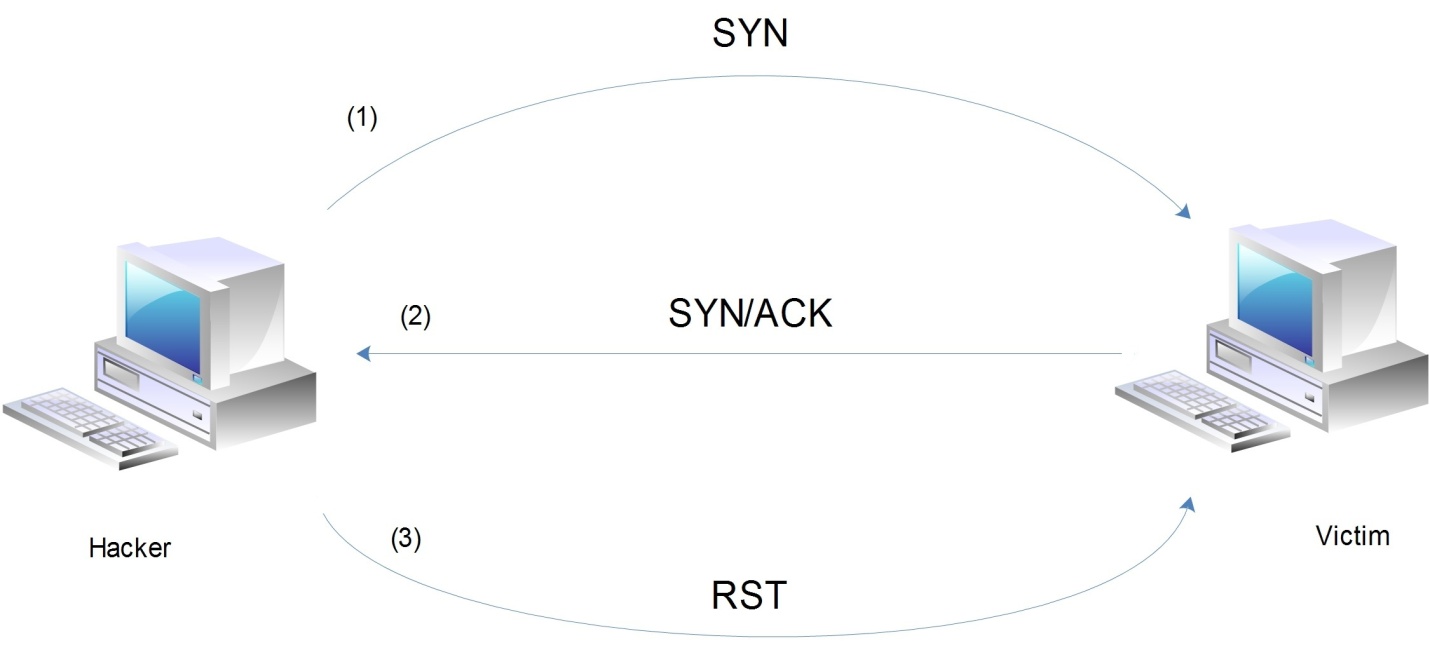


-Sau khi ta thiết lập và lưu lại thì khi 1 gói tin bất kì đi qua TMG sẽ bị chặn lại , sau đó thành phần “Packet Filtering” trong TMG sẽ tiến hành lọc gói tin theo thông số mà chúng ta vừa thiết lập , nếu gói tin thỏa mãn rule thì nó sẽ được thông qua , còn nếu gói tin của IP vi phạm thì sẽ bị chặn lại và hiện ra thông báo :



### 6.4. IP half-scan

**-** Đây là kĩ thuật dùng để quét các cổng của mục tiêu bằng cách sử dụng quá trình bắt tay 3 bước .Kẻ tấn công sẽ gửi một gói tin SYN đến tất cả các cổng của mục tiêu. Trong trường hợp các cổng tương ứng mở nó sẽ gửi trả lại một gói tin **SYN/ACK**. Tại thời điểm này kẻ tấn công sẽ kết thúc bằng một gói tin **RST**. Nếu cổng đóng, mục tiêu sẽ gửi trở lại một gói tin **RST**. Nhờ đó hacker sẽ biết được cổng nào đóng , mở .



Cách tấn công : Ta sử dụng công cụ nmap , để tấn công , ta gõ dòng lệnh sau trong cmd :

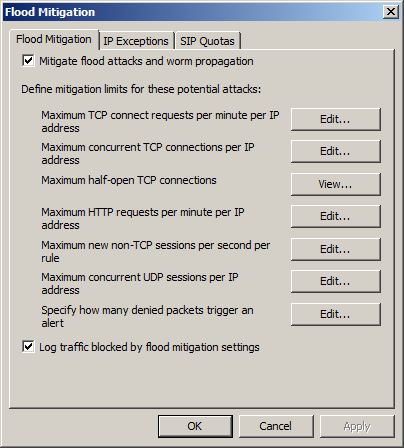
nmap –sS 192.168.2.2

Lệnh ta vừa gõ ở trên sẽ khiến cho công cụ Nmap tạo ra 65535 gói tin TCP để gửi tới 65535 port để kiểm tra coi địa chỉ 192.168.2.2 có cổng nào mở không , hoặc ta có thể dùng lệnh sau:

nmap -sS -p 22 192.168.2.2

Dùng lệnh này để kiểm tra coi địa chỉ 192.168.2.2 có mở cổng 22 hay không.

***-Phòng chống***:Để phòng chống phương pháp tấn công ở trên , ta mở TMG lên , sau đó chọn **Intrusion Prevention System**, sau đó chọn tab **Behavioral Intrusion Detection** trong cửa sổ chính và kích **Configure Flood Mitigation Settings . Sau đó tích vào ô Mitigate flood attacks and worm propagation, ta có hình dưới đây:**



Sau khi có bảng như trên đây , thì ta nhìn vào thông số dưới đây :

* Số kết nối half-open TCP tối đa. Ta có hình sau:

3.PNG

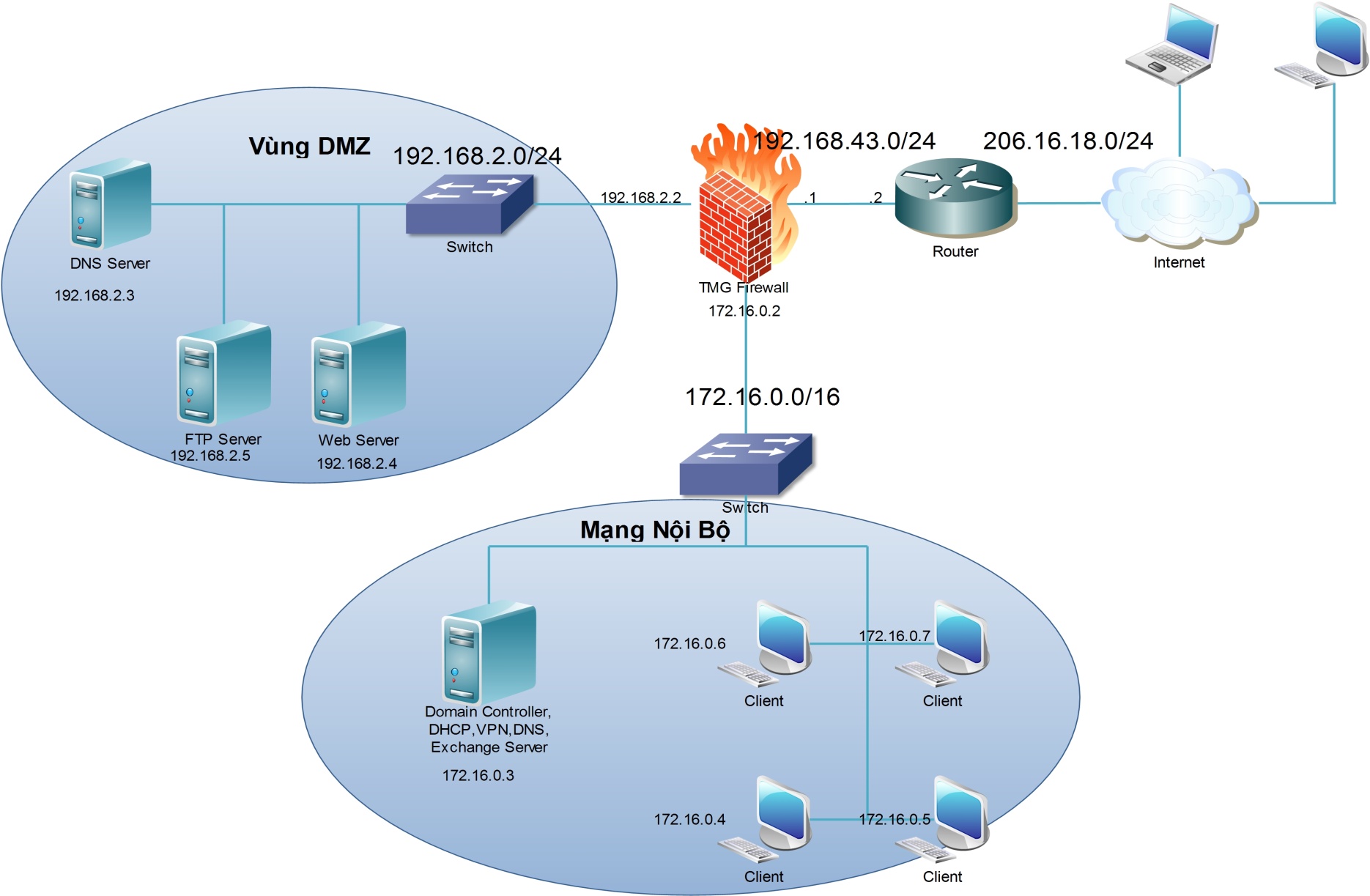
-Cái này là được thiết lập sẵn và không thể chỉnh sửa được. Khi 1 gói tin bất kì đi qua TMG sẽ bị chặn lại , sau đó thành phần “Packet Filtering” trong TMG sẽ tiến hành lọc gói tin theo thông số trên, nếu gói tin thỏa mãn rule thì nó sẽ được thông qua , còn nếu gói tin của IP vi phạm thì sẽ bị chặn lại và hiện ra thông báo :



# CHƯƠNG III.DEMO

## 1.Chức năng phát hiện và phòng chống tấn công trong TMG.

* **Sơ đồ :**

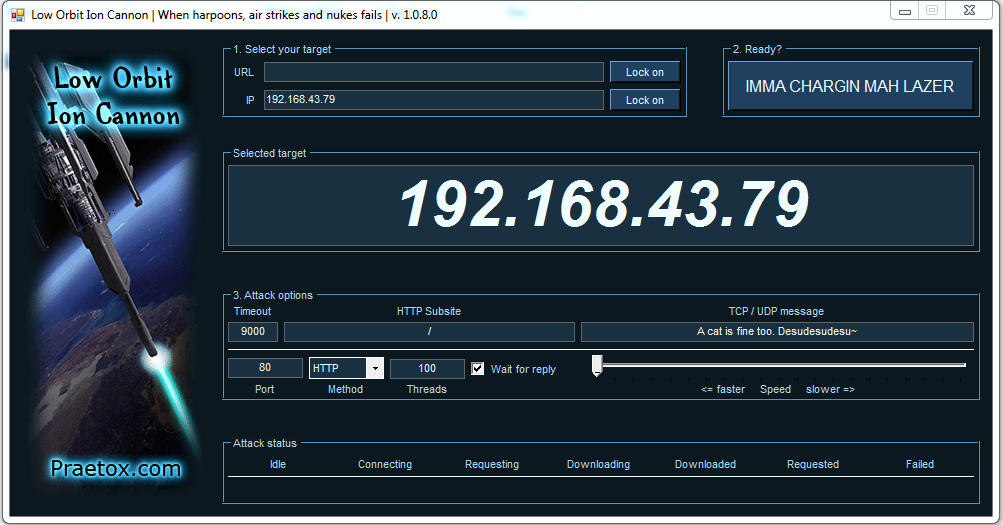


Sơ đồ TMG 2010 ứng dụng trong doanh nghiệp

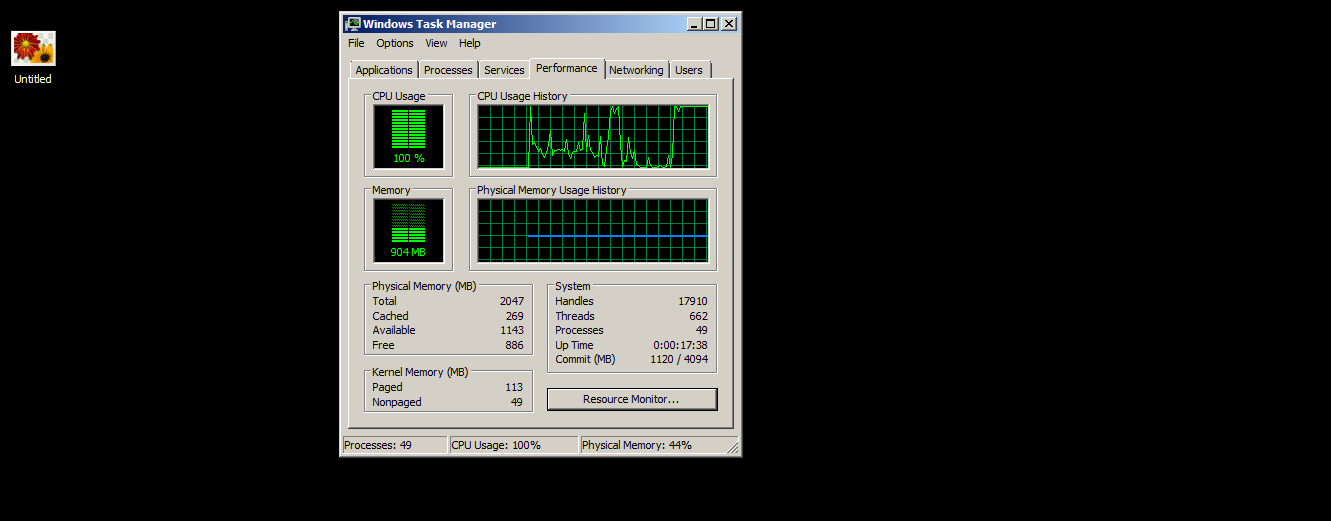
## 2. Các cuộc tấn công từ bên ngoài

### 2.1.HTTP Request

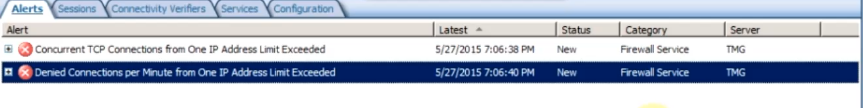
**-**Để tấn công , ta dùng công cụ LOIC và điền các thông số như sau:



-Sau khi kích hoạt tấn công thì máy chủ sẽ bị treo như sau :



-Nếu máy chủ có phần mềm tường lửa TMG thì nó sẽ tiến hành chặn gói tin và hiện ra cảnh báo sau:

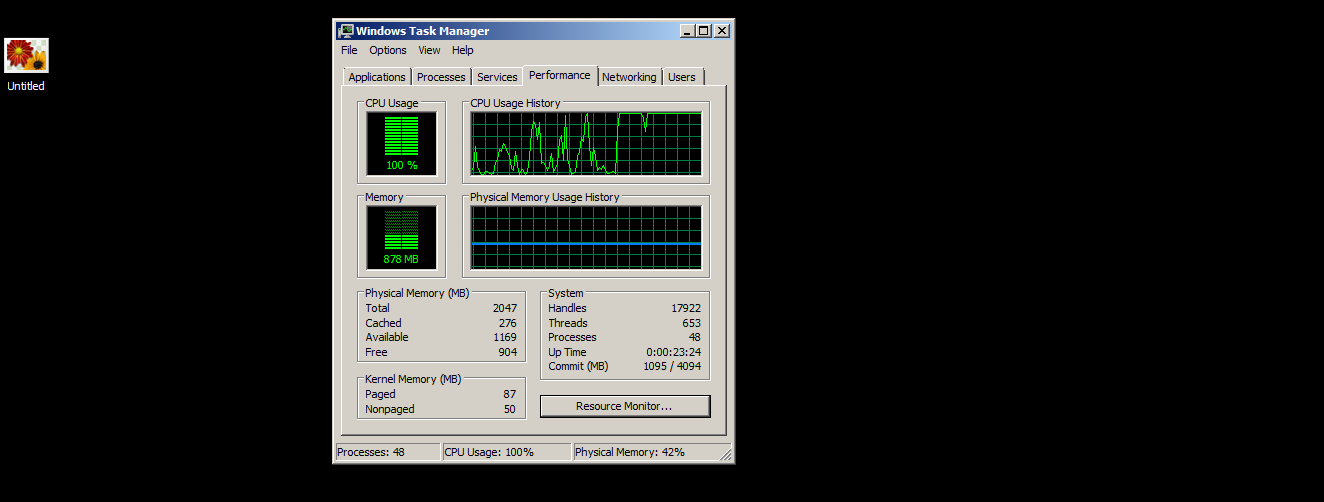


### 2.2.UDP Flood

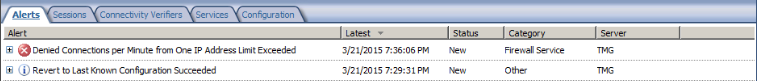
- Để tấn công , ta dùng công cụ “hping3” trong Backtrack5 như sau:

udp flood (new).PNG

-Sau khi kích hoạt tấn công thì máy chủ sẽ bị treo như sau :

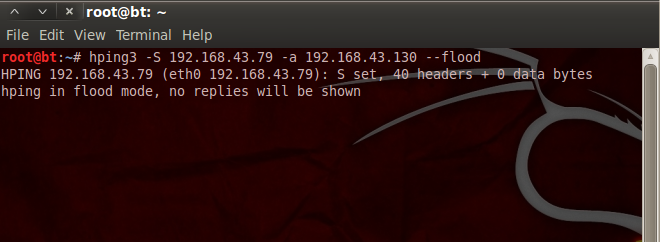


-Nếu máy chủ có phần mềm tường lửa TMG thì nó sẽ tiến hành chặn gói tin và hiện ra cảnh báo sau:

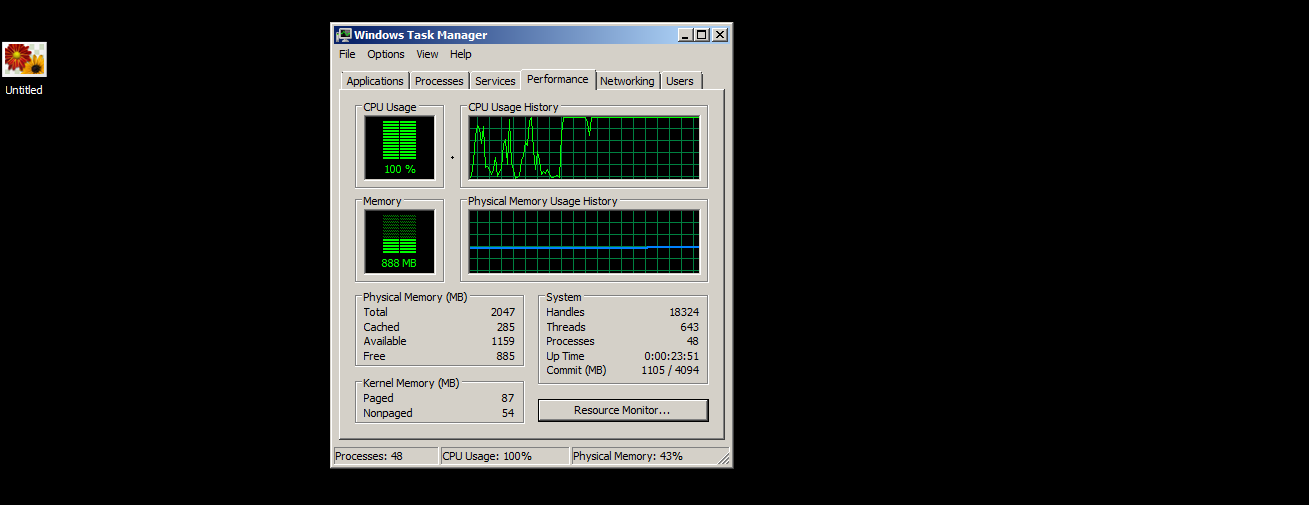


### 2.3.TCP SYN Flood

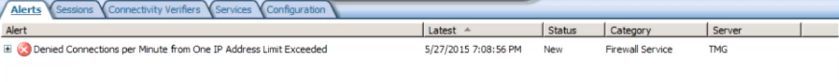
**-**Để tấn công , ta dùng công cụ “hping3” trong Backtrack5 như sau :



-Sau khi kích hoạt tấn công thì máy chủ sẽ bị treo như sau :



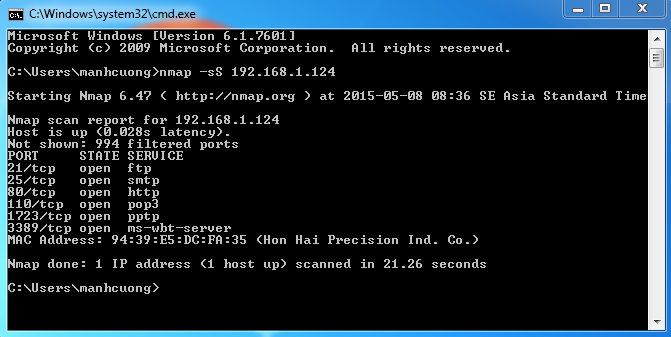
-Nếu máy chủ có phần mềm tường lửa TMG thì nó sẽ tiến hành chặn gói tin và hiện ra cảnh báo sau:



### 2.4.IP Half-scan

-Ta sử dụng công cụ nmap , để tấn công , ta gõ dòng lệnh sau trong cmd :

* nmap –sS 192.168.2.2



-Nếu máy chủ có phần mềm tường lửa TMG thì nó sẽ tiến hành chặn gói tin và hiện ra cảnh báo sau:



# CHƯƠNG IV.TỔNG KẾT

## 1.KẾT LUẬN

-Sau khi thực hiện đồ án “Xây Dựng Firewall TMG 2010 Trong Bảo Mật Mạng Doanh Nghiệp ” chúng em đã nắm vững được lí thuyết cũng như cách thức hoạt động của tường lửa TMG 2010.Những phần chúng em đã thực hiện thành công là :

* Cài đặt và cấu hình các chức năng chính.
* Thực hiện tấn công vô mạng nội bộ được bảo vệ bởi TMG 2010 và phát hiện và giảm thiểu được nó.

-Chúng em hi vọng rằng những kết quả mà chúng em nghiên cứu được sẽ góp phần là tài liệu bổ ích cho các bạn sinh viên khi nghiên cứu về Firewall nói chung cũng như tường lửa THREAT MANAGERMENT GATEWAY 2010nói riêng.

## 2.HƯỚNG PHÁT TRIỂN

-Ngày nay ,việc sử dụng internet đã quá phổ biến. Trong toàn bộ các doanh nghiệp, mọi nhân viên đều có 1 chiếc máy tính để truy cập internet để làm việc cũng như giải trí. Tuy nhiên việc quản lý chúng vẫn chưa được quan tâm đúng mức, chính điều này sẽ góp phần ảnh hưởng rất lớn đến hoạt động kinh doanh của công ty. Do đó việc trang bị tường lửa TMG 2010 cho mạng nội bộ doanh nghiệp là điều hết sức quan trọng.

-Trong phạm vi đồ án chúng em chỉ có thể trình bày những phần cơ bản nhất về tường lửa TMG 2010. Những điều này đã thực hiện tốt và có thể ứng dụng trong thực tế. Tuy nhiên vẫn còn có nhiều điểm cải tiến và nghiên cứu thêm như :

* Tìm hiểu việc làm tăng hiệu suất của TMG.
* Tìm hiểu việc gói tin sẽ đi đâu khi trong mạng có TMG.

**TÀI LIỆU THAM KHẢO**

* [1]<http://www.quantrimang.com.vn/phat-hien-va-ngan-chan-xam-nhap-trong-forefront-tmg-phan-2-nis-83315>
* [2]<http://nguyentanvy.wordpress.com/2011/11/28/cc-thnh-ph%E1%BA%A7n-c%E1%BB%A7a-firewall-v-c%C6%A1-ch%E1%BA%BF-ho%E1%BA%A1t-d%E1%BB%99ng/>
* [3]<http://www.quantrimang.com.vn/print/76487.aspx>
* [4]<http://echip.com.vn/tuong-lua-cho-he-thong-mang---cac-khai-niem-co-ban-a20130406070923659-c1110.html>
* [5]<http://www.wattpad.com/1458487-t%C3%ACm-hi%E1%BB%83u-v%E1%BB%81-firewall/page/2>
* [6]<http://diractionusa.com/store/_docs/product_descriptions/FfTMG2010.pdf>
* [7]Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion - Jim Harrison, Yuri Diogenes, Mohit Saxena, Tom Shinder