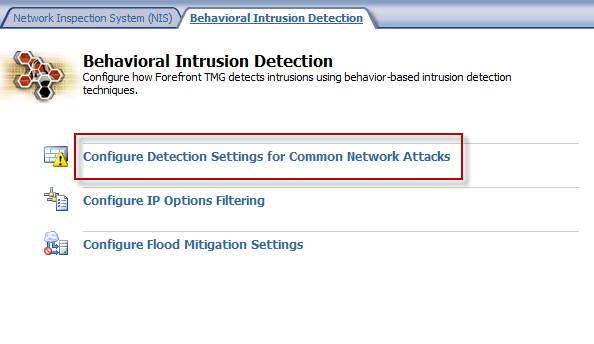
# Phát hiện và ngăn chặn xâm nhập trong Forefront TMG – Phần 1: Phát hiện hành vi

**Trong loạt bài gồm hai phần này, chúng tôi sẽ giới thiệu cho các bạn về các tính năng phát hiện hành vi của Forefront TMG.**

Microsoft Forefront Threat Management Gateway (TMG) 2010 là một hệ thống phòng chống vành đai đa lớp gồm nhiều công nghệ bảo vệ nâng cao. Ngoài việc tích hợp tính năng lọc URL, quét virus, mã độc và thanh tra HTTPS, TMG firewall còn có khả năng phát hiện và ngăn chặn xâm nhập. Trong phần một của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn tính năng ngăn chặn và phát hiện xâm phạm dựa trên hành vi. Phần hai sẽ giới thiệu về Network Inspection System (NIS), cung cấp tính năng ngăn chặn và phát hiện xâm nhập dựa trên lỗ hổng.

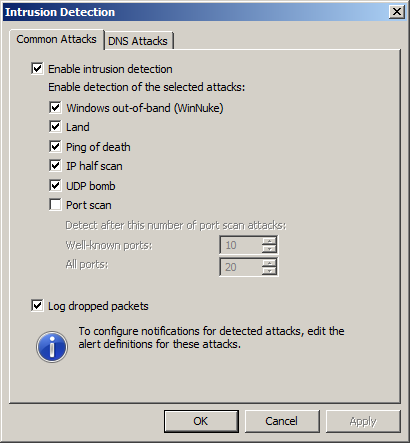
**Những tấn công mạng phổ biến**

Tính năng phát hiện và ngăn chặn xâm nhập trong Forefront TMG được xây dựng dựa trên tính năng phát hiện và ngăn chặn xâm nhập dựa trên hành vi có trong Microsoft ISA Server 2000. Bằng cách thực hiện thanh tra gói dữ liệu ở mức thấp, TMG firewall có thể phát hiện và khóa chặn nhiều kiểu tấn công. Khả năng phát hiện và ngăn chặn xâm nhập được cấu hình bằng cách mở TMG management console, đánh dấu **Intrusion Prevention System**, sau đó chọn tab **Behavioral Intrusion Detection** trong cửa sổ điều khiển chính và kích**Configure Detection Settings for Common Network Attacks**.

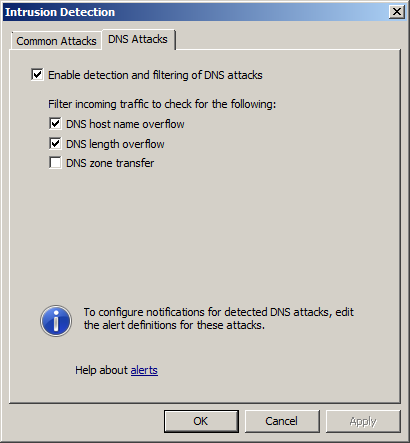
  
Hình 1

Ở đây bạn sẽ thấy tính năng phát hiện xâm nhập được kích hoạt và được cấu hình mặc định để nhận diện, khóa chặn cũng như ghi chép các tấn công dưới đây:

* Windows out-of-band (WinNuke)
* Land
* Ping of death
* IP half scan
* UDP bomb
* Port scan (không được kích hoạt mặc định)

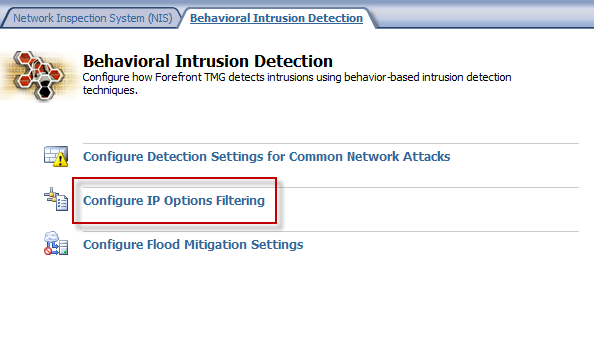
  
Hình 2

Ngoài ra, bằng cách chọn tab **DNS Attacks**, bạn sẽ thấy TMG firewall cũng có khả năng cung cấp tùy chọn bảo vệ lớp ứng dụng nâng cao dành cho nhiều tấn công phổ biến nhắm tới các máy chủ DNS công cộng, chẳng hạn như **DNS hostname overflow** và **DNS length overflow**. TMG firewall có thể ngăn chặn việc xảy ra hiện tượng chuyển vùng DNS (tuy nhiên không được kích hoạt mặc định).

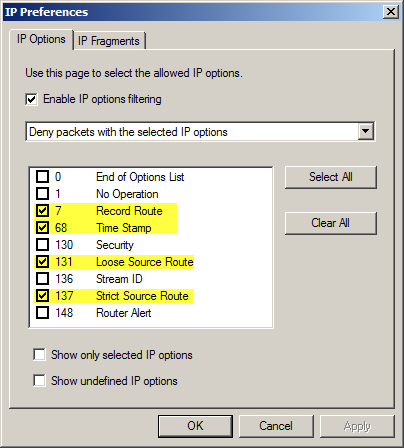
  
Hình 3

**Lọc IP option**

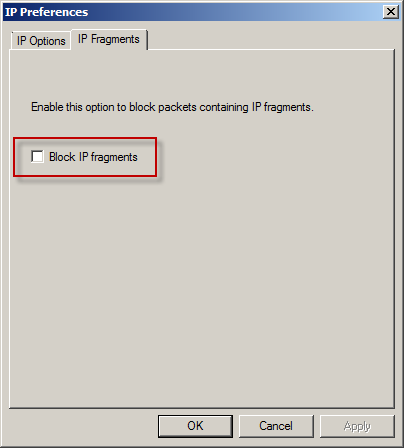
Tính năng phát hiện và ngăn chặn xâm nhập trong Forefront TMG cũng cho phép lọc *IP option* có trong header của một gói IP. Việc lọc *IP option* được kích hoạt mặc định và có thể được cấu hình bằng cách kích liên kết**Configure IP Options Filtering** trong cửa sổ điều khiển chính.

  
Hình 4

Hầu hết số *IP option* đều vô hại. Mặc dù vậy, vẫn có một số *IP option* chỉ thị dấu hiệu của hành vi mã độc tiềm tàng. Mặc định, TMG firewall được cấu hình để cho phép lọc *IP option* và sẽ bỏ các gói IP có chứa các *IP option*7 (Record Route), 68 (Time Stamp), 131 (Loose Source Route) và137 (Strict Source Route). Nếu gói IP đã kích hoạt các số option cụ thể, quản trị viên TMG firewall có thể điều chỉnh hành động diễn ra. Bất cứ gói nào có chứa *IP option*đều có thể bị bỏ qua, các gói với số *IP option* được chọn có thể bị từ chối hoặc tất cả các gói ngoại trừ số có *IP option* đã chọn sẽ bị từ chối.

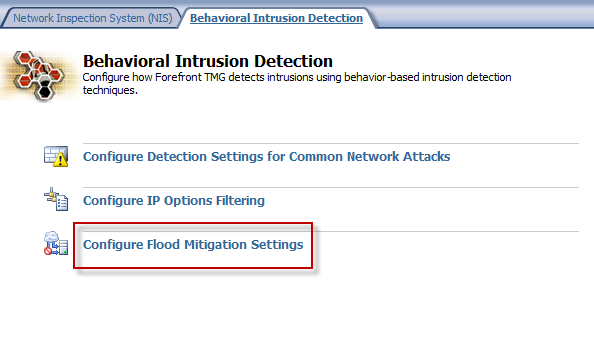
  
Hình 5

TMG firewall cũng có thể ngăn chặn việc chuyển tiếp gói dữ liệu có chứa các IP fragment. Tùy chọn này không được kích hoạt mặc định. Việc khóa chặn các IP fragment có thể gây những ảnh hưởng không mong muốn, vì vậy cần lưu ý khi kích hoạt tính năng này.

  
Hình 6

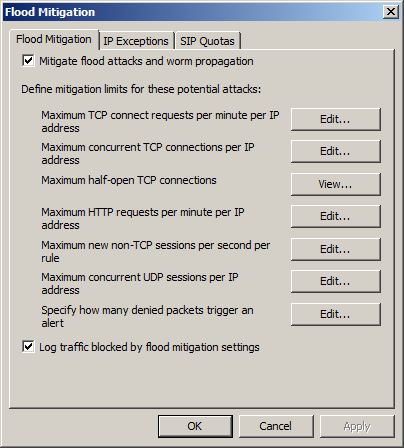
**Flood Mitigation**

Flood mitigation là một thành phần quan trọng của Forefront TMG firewall. Tính năng này giúp giảm nhẹ sự ảnh hưởng của một số kiểu tấn công trên tường lửa. Giúp giảm nhẹ các tấn công DoS tiềm tàng bằng cách thực thi một số hạn chế trên số lưu lượng mà một host có thể tạo. Flood mitigation được kích hoạt mặc định và có thể được cấu hình bằng cách kích liên kết **Configure Flood Mitigation Settings** trong cửa sổ điều khiển chính.

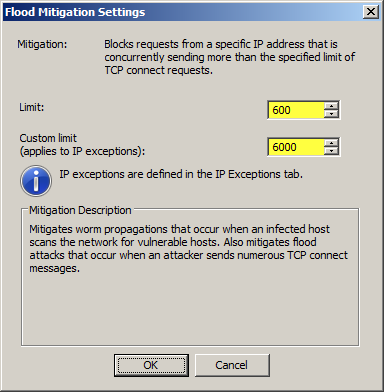
  
Hình 7

Flood mitigation có thể điều khiển các tham số mạng sau:

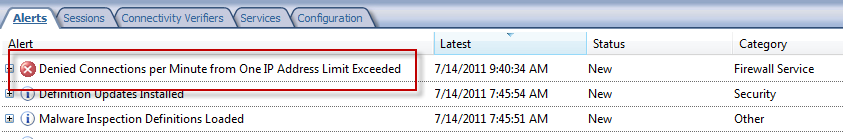
* Yêu cầu kết nối TCP tối đa trên phút trên một IP
* Tối đa số kết nối TCP đồng thời trên địa chỉ IP
* Kết nối half-open TCP lớn nhất
* Yêu cầu HTTP tối đa trên phút trên địa chỉ IP
* Non-TCP session mới tối đa trên giây trên một rule
* Tối đa số UDP session đồng thời trên một IP

  
Hình 8

Kích **Edit…**bên cạnh các tham số flood mitigation sẽ cho phép quản trị viên cấu những hạn chế kết nối để áp dụng cho IP exception.

  
Hình 9

Khi một host tạo đủ lượng lượng để vượt quá những hạn chế đã được đặt trước, TMG firewall sẽ bắt đầu bỏ rơi các gói từ host này và tạo cảnh báo.

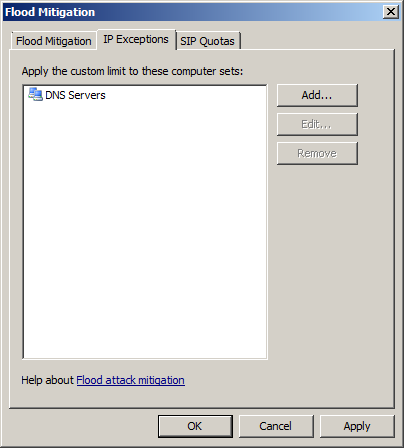
  
Hình 10

**Lưu ý:**

Một điều quan trọng cần lưu ý là sự truyền thông được phép bằng cách đếm đến hạn ngạch kết nối.

Nếu host đang được nói đến này ngừng gửi yêu cầu, hoặc giảm tần suất các yêu cầu được phát ra từ nó đến mức dưới giới hạn được thiết lập, sau một phút, tường lửa TMG firewall sẽ tăng sự cho phép các kết nối mới đến từ host này.

Thông thường, khi một host vượt quá giới hạn kết nối, nó sẽ bị nghi ngờ là lưu lượng mã độc hoặc có thể là một ứng dụng được viết kém chất lượng. Mặc dù vậy vẫn có một số trường hợp host tạo số lượng rất lớn lưu lượng hợp lệ. Một số ví dụ như DNS server và SMTP server. Tuy nhiên, một số quản trị viên sẽ có gắng giải quyết các vấn đề này bằng cách thêm hạn chế kết nối mặc định, hoặc thậm chí vô hiệu hóa hoàn toàn flood mitigation. Cách làm này không được khuyến khích. Cách xử lý phù hợp với kịch bản này là tạo một **IP exception**, sau đó thực thi một ngưỡng hạn chế nào đó cho các hệ thống rơi vào nhóm đối tượng này.

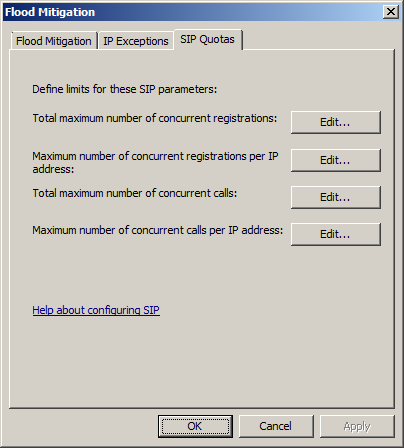
  
Hình11

**Hạn ngạch SIP**

Với sự xuất hiện của SIP filter trong TMG 2010, tường lửa hiện có khả năng thực thi các hạn ngạch đối với lưu lượng SIP. TMG đặt các hạn chế trên các tham số SIP sau:

* Tổng số đăng ký lớn nhất
* Số đăng ký đồng thời lớn nhất trên mỗi IP
* Tổng số cuộc gọi đồng thời lớn nhất
* Số cuộc gọi đồng thời lớn nhất trên mỗi IP

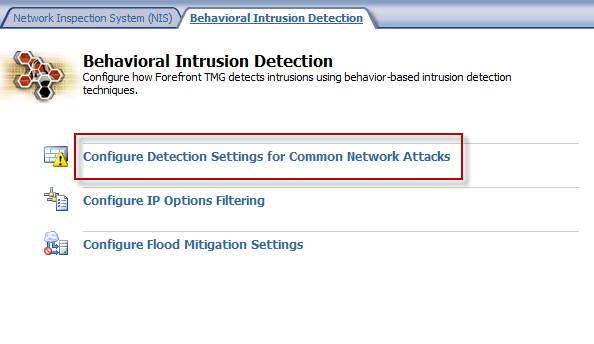
Kích **Edit…** bên cạnh mỗi tham số sẽ cho phép quản trị viên cấu hình các ngưỡng theo yêu cầu của mình.



# Phát hiện và ngăn chặn xâm nhập trong Forefront TMG – Phần 2: NIS

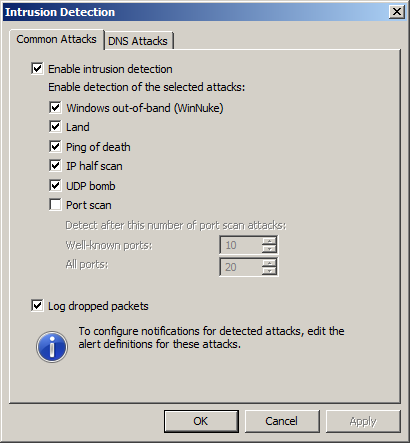
**Những tấn công mạng phổ biến**

Tính năng phát hiện và ngăn chặn xâm nhập trong Forefront TMG được xây dựng dựa trên tính năng phát hiện và ngăn chặn xâm nhập dựa trên hành vi có trong Microsoft ISA Server 2000. Bằng cách thực hiện thanh tra gói dữ liệu ở mức thấp, TMG firewall có thể phát hiện và khóa chặn nhiều kiểu tấn công. Khả năng phát hiện và ngăn chặn xâm nhập được cấu hình bằng cách mở TMG management console, đánh dấu **Intrusion Prevention System**, sau đó chọn tab **Behavioral Intrusion Detection** trong cửa sổ điều khiển chính và kích**Configure Detection Settings for Common Network Attacks**.

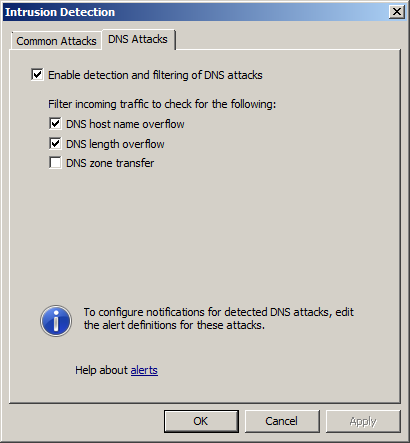
  
Hình 1

Ở đây bạn sẽ thấy tính năng phát hiện xâm nhập được kích hoạt và được cấu hình mặc định để nhận diện, khóa chặn cũng như ghi chép các tấn công dưới đây:

* Windows out-of-band (WinNuke)
* Land
* Ping of death
* IP half scan
* UDP bomb
* Port scan (không được kích hoạt mặc định)

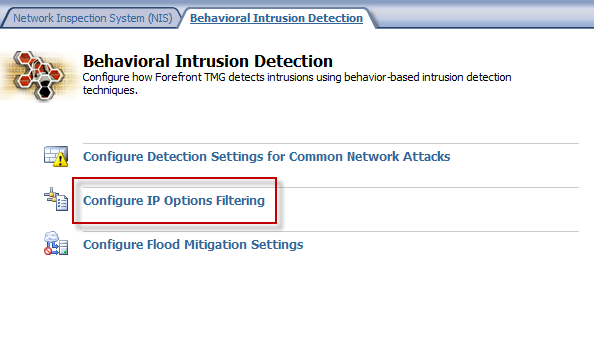
  
Hình 2

Ngoài ra, bằng cách chọn tab **DNS Attacks**, bạn sẽ thấy TMG firewall cũng có khả năng cung cấp tùy chọn bảo vệ lớp ứng dụng nâng cao dành cho nhiều tấn công phổ biến nhắm tới các máy chủ DNS công cộng, chẳng hạn như **DNS hostname overflow** và **DNS length overflow**. TMG firewall có thể ngăn chặn việc xảy ra hiện tượng chuyển vùng DNS (tuy nhiên không được kích hoạt mặc định).

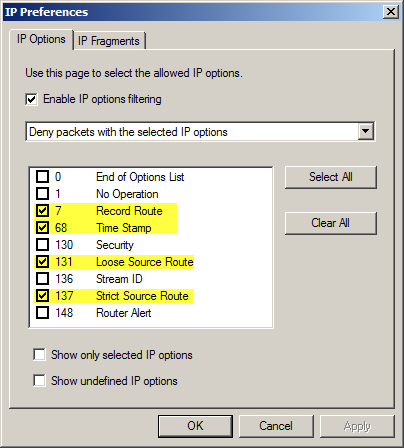
  
Hình 3

**Lọc IP option**

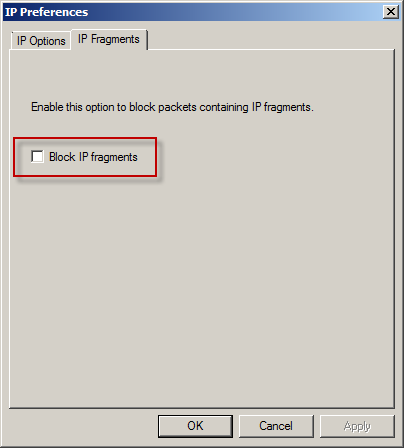
Tính năng phát hiện và ngăn chặn xâm nhập trong Forefront TMG cũng cho phép lọc *IP option* có trong header của một gói IP. Việc lọc *IP option* được kích hoạt mặc định và có thể được cấu hình bằng cách kích liên kết**Configure IP Options Filtering** trong cửa sổ điều khiển chính.

  
Hình 4

Hầu hết số *IP option* đều vô hại. Mặc dù vậy, vẫn có một số *IP option* chỉ thị dấu hiệu của hành vi mã độc tiềm tàng. Mặc định, TMG firewall được cấu hình để cho phép lọc *IP option* và sẽ bỏ các gói IP có chứa các *IP option*7 (Record Route), 68 (Time Stamp), 131 (Loose Source Route) và137 (Strict Source Route). Nếu gói IP đã kích hoạt các số option cụ thể, quản trị viên TMG firewall có thể điều chỉnh hành động diễn ra. Bất cứ gói nào có chứa *IP option*đều có thể bị bỏ qua, các gói với số *IP option* được chọn có thể bị từ chối hoặc tất cả các gói ngoại trừ số có *IP option* đã chọn sẽ bị từ chối.

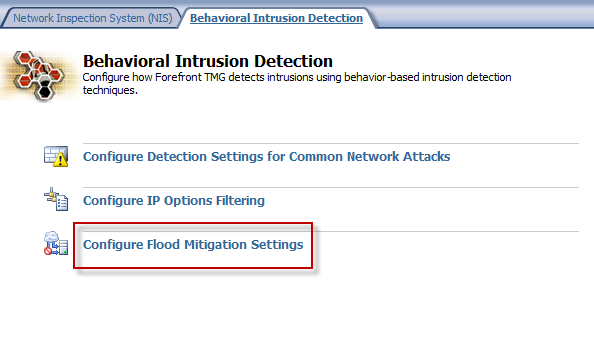
  
Hình 5

TMG firewall cũng có thể ngăn chặn việc chuyển tiếp gói dữ liệu có chứa các IP fragment. Tùy chọn này không được kích hoạt mặc định. Việc khóa chặn các IP fragment có thể gây những ảnh hưởng không mong muốn, vì vậy cần lưu ý khi kích hoạt tính năng này.

  
Hình 6

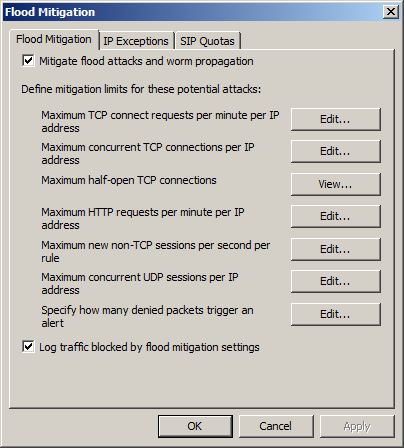
**Flood Mitigation**

Flood mitigation là một thành phần quan trọng của Forefront TMG firewall. Tính năng này giúp giảm nhẹ sự ảnh hưởng của một số kiểu tấn công trên tường lửa. Giúp giảm nhẹ các tấn công DoS tiềm tàng bằng cách thực thi một số hạn chế trên số lưu lượng mà một host có thể tạo. Flood mitigation được kích hoạt mặc định và có thể được cấu hình bằng cách kích liên kết **Configure Flood Mitigation Settings** trong cửa sổ điều khiển chính.

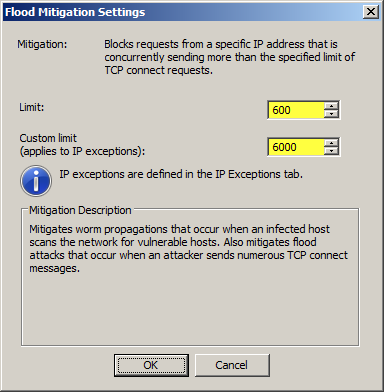
  
Hình 7

Flood mitigation có thể điều khiển các tham số mạng sau:

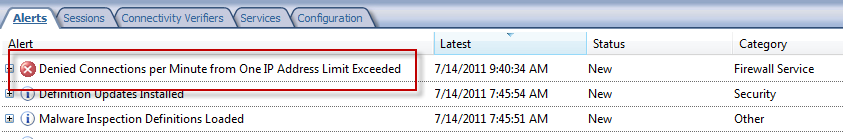
* Yêu cầu kết nối TCP tối đa trên phút trên một IP
* Tối đa số kết nối TCP đồng thời trên địa chỉ IP
* Kết nối half-open TCP lớn nhất
* Yêu cầu HTTP tối đa trên phút trên địa chỉ IP
* Non-TCP session mới tối đa trên giây trên một rule
* Tối đa số UDP session đồng thời trên một IP

  
Hình 8

Kích **Edit…**bên cạnh các tham số flood mitigation sẽ cho phép quản trị viên cấu những hạn chế kết nối để áp dụng cho IP exception.

  
Hình 9

Khi một host tạo đủ lượng lượng để vượt quá những hạn chế đã được đặt trước, TMG firewall sẽ bắt đầu bỏ rơi các gói từ host này và tạo cảnh báo.

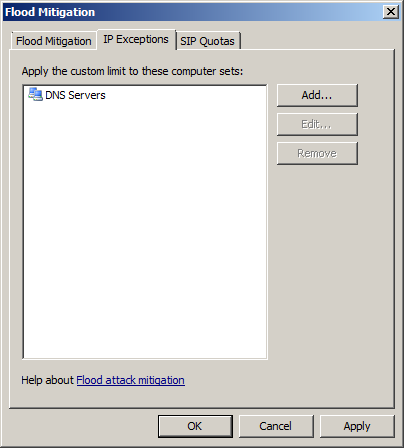
  
Hình 10

**Lưu ý:**

Một điều quan trọng cần lưu ý là sự truyền thông được phép bằng cách đếm đến hạn ngạch kết nối.

Nếu host đang được nói đến này ngừng gửi yêu cầu, hoặc giảm tần suất các yêu cầu được phát ra từ nó đến mức dưới giới hạn được thiết lập, sau một phút, tường lửa TMG firewall sẽ tăng sự cho phép các kết nối mới đến từ host này.

Thông thường, khi một host vượt quá giới hạn kết nối, nó sẽ bị nghi ngờ là lưu lượng mã độc hoặc có thể là một ứng dụng được viết kém chất lượng. Mặc dù vậy vẫn có một số trường hợp host tạo số lượng rất lớn lưu lượng hợp lệ. Một số ví dụ như DNS server và SMTP server. Tuy nhiên, một số quản trị viên sẽ có gắng giải quyết các vấn đề này bằng cách thêm hạn chế kết nối mặc định, hoặc thậm chí vô hiệu hóa hoàn toàn flood mitigation. Cách làm này không được khuyến khích. Cách xử lý phù hợp với kịch bản này là tạo một **IP exception**, sau đó thực thi một ngưỡng hạn chế nào đó cho các hệ thống rơi vào nhóm đối tượng này.

  
Hình11

**Hạn ngạch SIP**

Với sự xuất hiện của SIP filter trong TMG 2010, tường lửa hiện có khả năng thực thi các hạn ngạch đối với lưu lượng SIP. TMG đặt các hạn chế trên các tham số SIP sau:

* Tổng số đăng ký lớn nhất
* Số đăng ký đồng thời lớn nhất trên mỗi IP
* Tổng số cuộc gọi đồng thời lớn nhất
* Số cuộc gọi đồng thời lớn nhất trên mỗi IP

Kích **Edit…** bên cạnh mỗi tham số sẽ cho phép quản trị viên cấu hình các ngưỡng theo yêu cầu của mình.

