Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Microsoft Forefront TMG Behavioral Intrusion Detection

Abstract

In this article, I will show you how Microsoft Forefront TMG protects itself and the networks behind it against external intruders and malicious attacks.

Let's begin

First, keep in mind that the information in this article are based on a beta version of Microsoft Forefront TMG and are subject to change.

A few months ago, Microsoft released Beta 3 of Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

One of the strength of Microsoft Forefront TMG is to protect against several network attacks and intrusion attempts.
Beginning with Microsoft Forefront TMG, Microsoft has divided these defense mechanisms into two parts:

- Network Inspection System (NIS)
- Behavioral Intrusion Detection

While many parts of the behavioral Intrusion Detection already exist in ISA Server 2006, the Network Inspection System (NIS) is new in Microsoft Forefront TMG. If you want to learn more about NIS, please read our articles regarding NIS at www.isaserver.org. This article focuses on Behavioral Intrusion Detection.

Behavioral Intrusion Detection

Most parts of the Behavioral Intrusion Detection mechanism in TMG are not new and remain unchanged in TMG comparing against ISA Server 2006.

TMG comes with the following behavioral Intrusion Detection mechanism:

- Common Network attacks
- IP options filtering
- Flood Mitigation

Before we start explaining the different settings, I will try to give you a short overview about common type of attacks to give you some background information.

Some type of Attacks

To know how "Hackers" are working, you need to know about the art of hacking and which type of attacks exists. The following table will give you an overview about some type of attacks.

Attack	Description
Internal worm attack over a TCP connection	Clients will be infected from the worm and now they try to distribute the worm over different ports to other computers on the network
Connection table exploit	An Attacker tries to fill the connection table with bad requests, so that ISA server cannot fulfil legitimate requests
Sequential TCP connections during flood attack	An Attacker tries to sequentially open and intermediately closing many TCP connections to bypass the quota mechanism to consume a lot of ISA resources
Hypertext Transfer Protocol (HTTP) DDoS using existing connections	An Attacker sends an excessive amount of HTTP requests through an existing TCP connection which used the Keep alive interval

Configure Detection settings for Common Network Attacks

The Common Attacks settings allows you to configure some basic intrusion detection methods against several known attacks.

Common Attacks

Common attacks are a Ping of Death, UDP bombs or IP half scans and some more. This protection mechanisms are not new, but should be a basic recommended setting for most TMG servers.

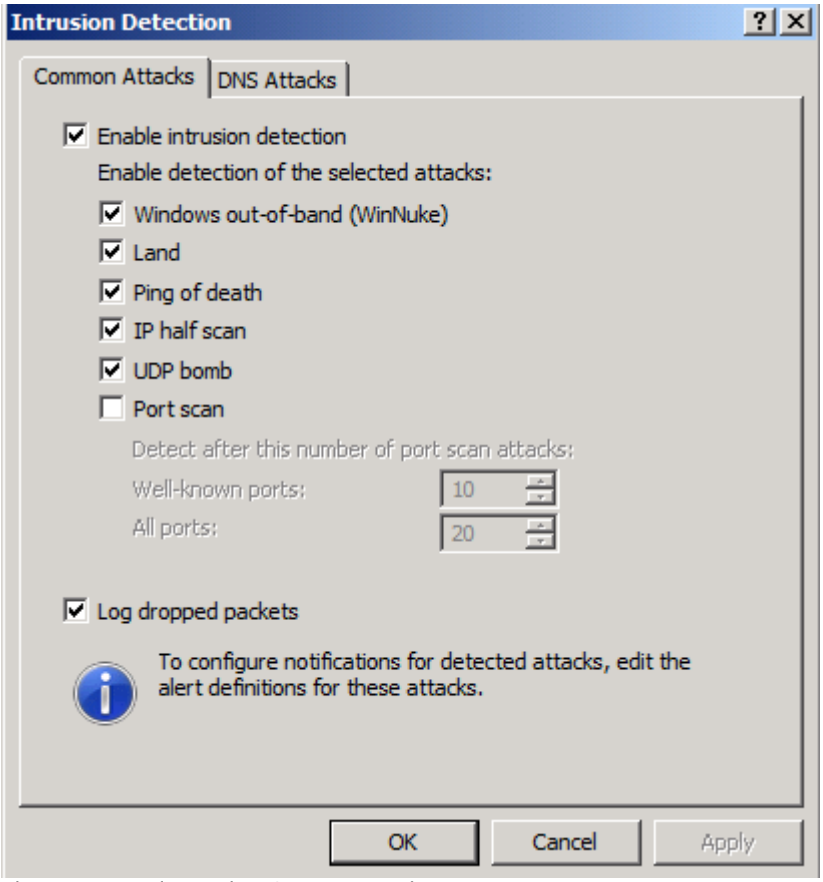

Figure 1: Protecting against Common Attacks

Per default, Microsoft Forefront TMG logs all dropped packets to get informed when an intruder tries to connect to the Firewall.

DNS Attacks

Forefront TMG allows you to configure the Firewall to filter DNS traffic with an builtin DNS-Filter. TMG protects against DNS host name overflow, DNS length overflow and if necessary it filters DNS zone transfer data. If you activate the DNS zone transfer option, TMG denies a possible DNS zone transfer through the Firewall.

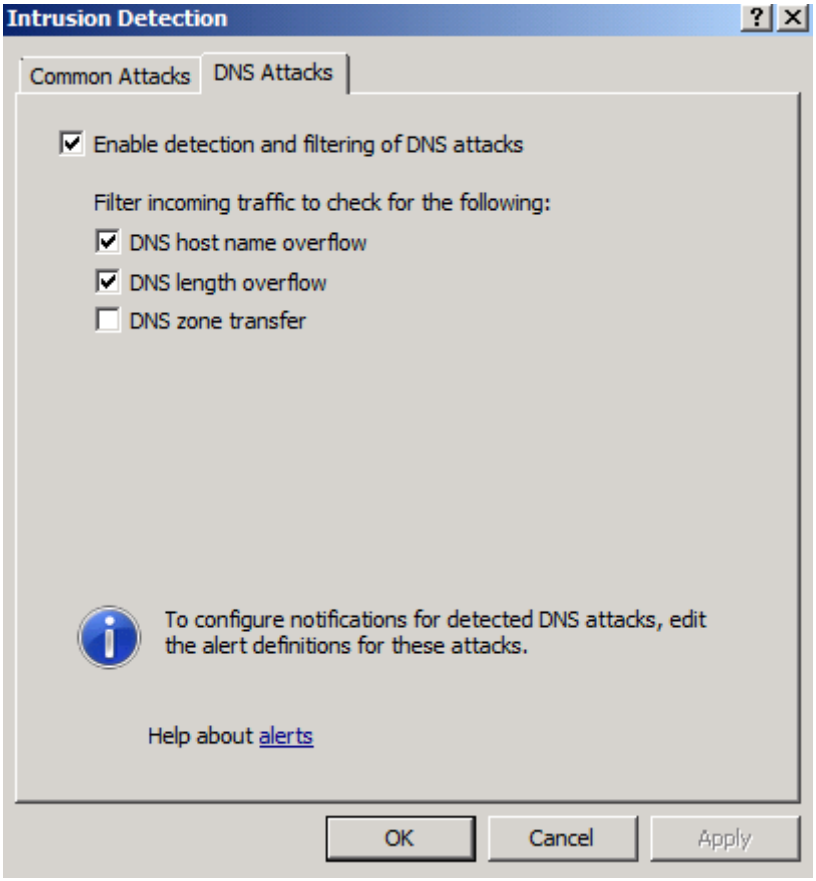

Figure 2: Protecting against DNS attacks

Configure IP Options Filtering

After we had finished explaining the common attacks options, we should have a look at the IP options filtering in Forefront TMG.

IP Options

The TCP/IP protocol defines several IP options which can be used for several purposes in IP networking. Microsoft Forefront TMG has the capability to block some IP options because not all IP options are used today in IP networking and some IP options might be used to infiltrate the network. Per default TMG denies some IP options as you can see in the following screenshot and it is up to you to deny IP options which you don't want to use, but be carefully which IP options you deactivate because a wrong setting can cause several network failures.

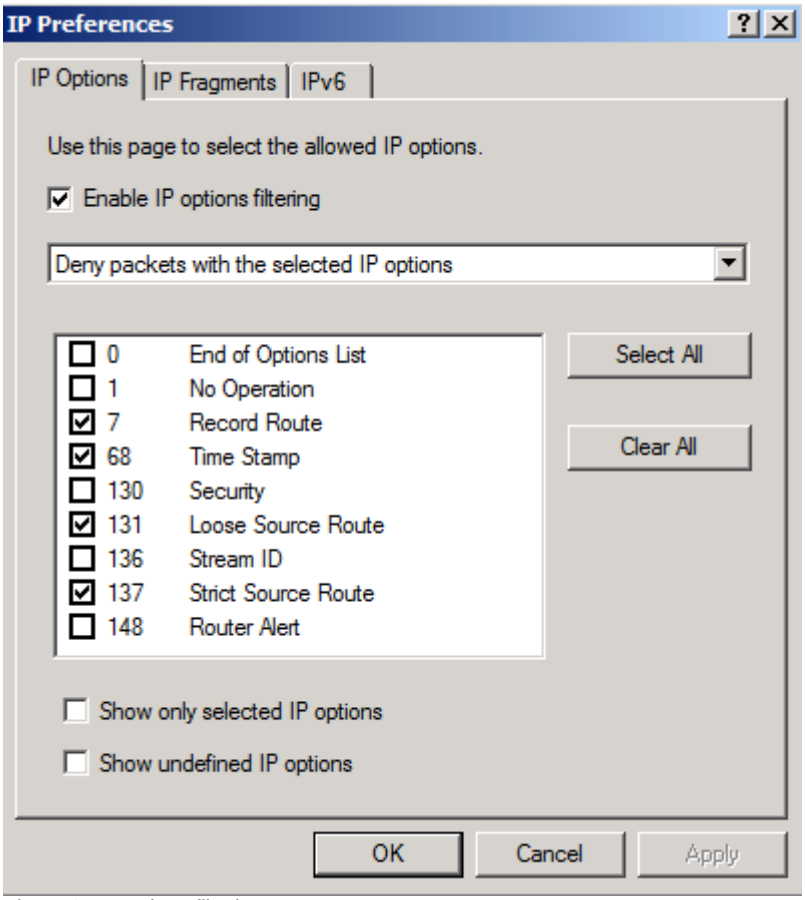

Figure 3: IP options filtering

IP Fragments

Microsoft Forferont TMG allows you to block IP Fragments. IP fragmentation is used to fragement packets if they are larger than the configured maximum size. This setting is disabled by default and you should carefully activate this feature becaus it could break VPN connections and some other traffic.

IPv6

This is a new setting in Microsoft Forefront TMG. Because Microsoft Forefront TMG can be used in conjunction with the new Direct Access (DA) feature of Windows Server 2008 R2, you must manually allow TMG Server to act as a Direct Access Server. For more informations about Direct Access follow the link in the Link section at the end of this article.

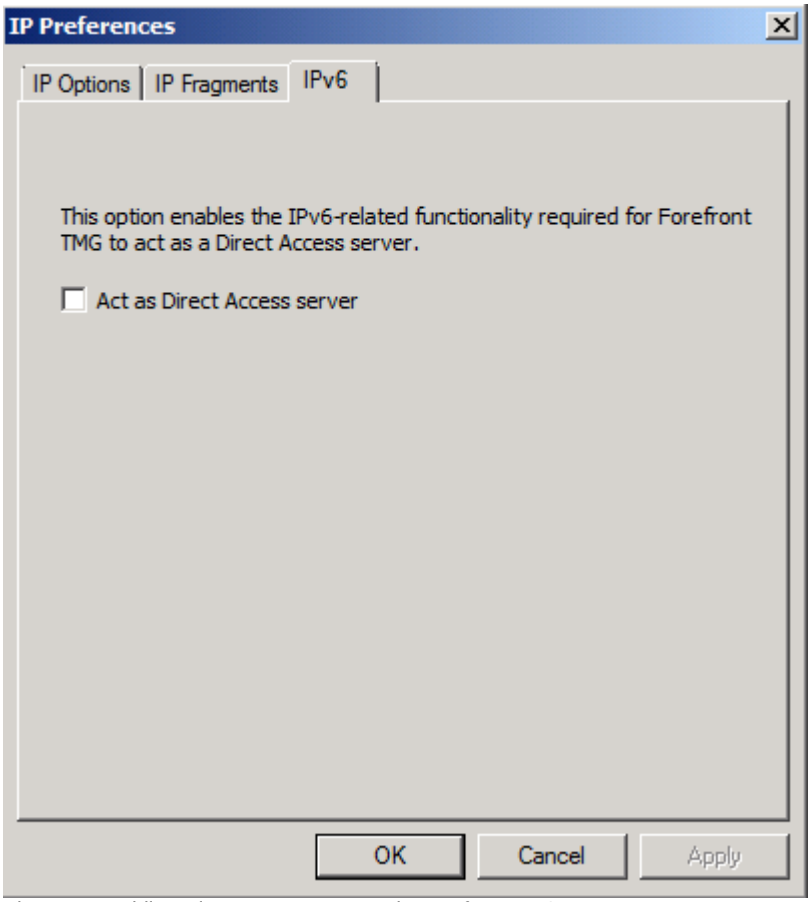

Figure 4: Enabling Direct Access support in Forefront TMG

Configure Flood Mitigation Settings

Microsoft Forefront TMG includes some attack mitigation features which you can configure and monitor with the Microsoft forefront TMG management console. The settings in TMG are almost the same as in ISA Server 2006, so if you are familiar with the configuration in ISA Server 2006, you wouldn't have problems with these features in TMG. TMG contains the following features:

- HTTP connection limits
- Flood Attack and Worm propagation features
- Limit the number of concurrent users
- Protection against specific attacks like IP spoofing, DNS overflows, DHCP poisoning and intrusion detection

Flood Attack and Worm Propagation Mitigation

A flood attacks is defined as an attack from a malicious user when this user tries to flood a machine or a network with garbage TCP packets. A flood attack may cause one of the following reactions:

- Heavy disk load and resource consumption on the firewall
- High CPU load
- High memory consumption
- High network bandwidth consumption

With Microsoft Forefront TMG it is possible to set a maximum number of connections during a defined time period or a maximum of connections for an IP address. When the number of maximum client requests has reached, any new client requests are denied and connections are dropped.

The default configuration settings of Flood Mitigation in Microsoft Forefront TMG help to ensure that TMG Server can continue to function, even when TMG is under a flood attack.

Attack	TMG Mitigation	Defaults
Flood attack. A specific IP address tries to open many connections to many different IP addresses to create a flood attack	TCP connect requests per minute, per IP address	By default, TMG Server limits the number of TCP requests per client to 600 per minute. Keep in mind that there are some legitimate applications that could create a high number of connection attempts
Flood attack. A specific IP address tries to flood ISA Server by maintaining numerous TCP connections concurrently	Concurrent TCP connections per IP address	TMG limits the number of TCP concurrent connections per client to 160
SYN attack. A malicious client tries to flood TMG Server with a large amount of half-open TCP connections	TMG mitigates SYN attacks.	TMG limits the number of concurrent half-open TCP connections to half the number of concurrent connections configured for concurrent TCP connections. This setting cannot be changed
User Datagram Protocol (UDP) flood attack. A IP address tries to start a denial of service attack	UDP concurrent sessions per IP address. When a UDP flood attack occurs, TMG Server closes older sessions, so that no more than the specified number of connections is allowed concurrently	TMG limits the number of concurrent UDP sessions per IP address to 160. This limit is configurable to 400 concurrent UDP sessions

Flood attack configuration

Let’s start with some basic steps to configure Flood Mitigation in the TMG Server Management console.

In the configure Flood Mitigation settings it is possible to enable the mitigation against flood and worm propagation and the setting if blocked traffic should be logged.

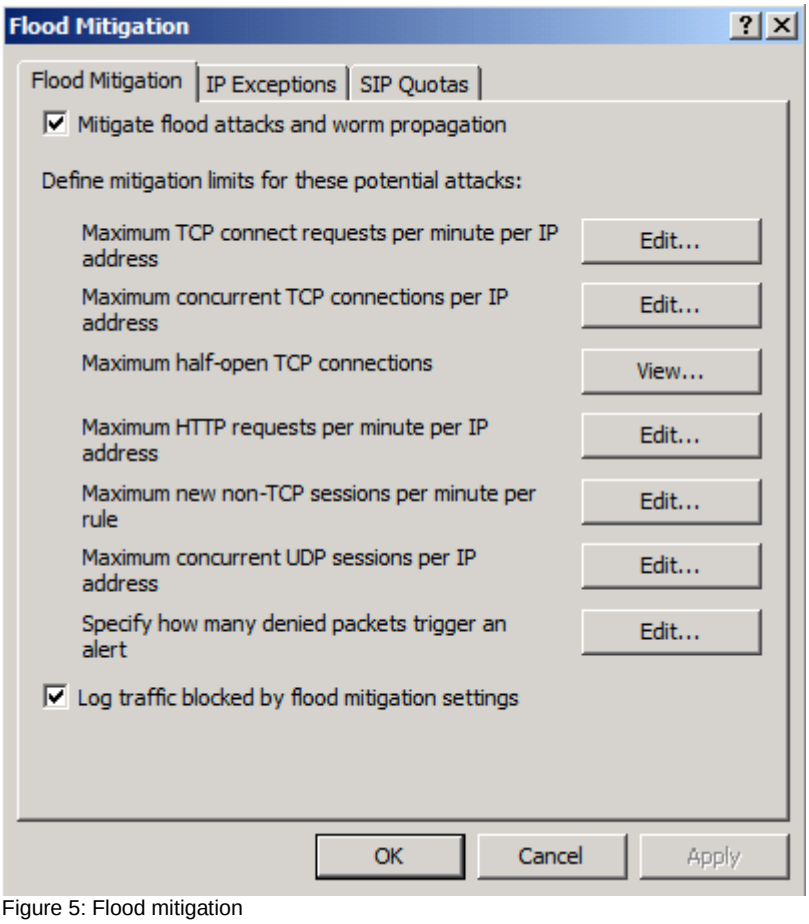

Figure 5: Flood mitigation

For a lot of flood mitigation settings it is possible to configure custom limits for specific IP addresses from which you know that theses IP addresses are not compromised and the traffic is legitimate.

IP exceptions

Not every attack is a real attack from a hacker or malicious user. There are some legal reasons for a client which creates more connections at a time or IP address as other clients. After clarifying that the client has a legal reason for so much traffic and you are sure that TMG has enough resources for additional connections, it is possible to create IP exceptions as shown in the following screenshot.

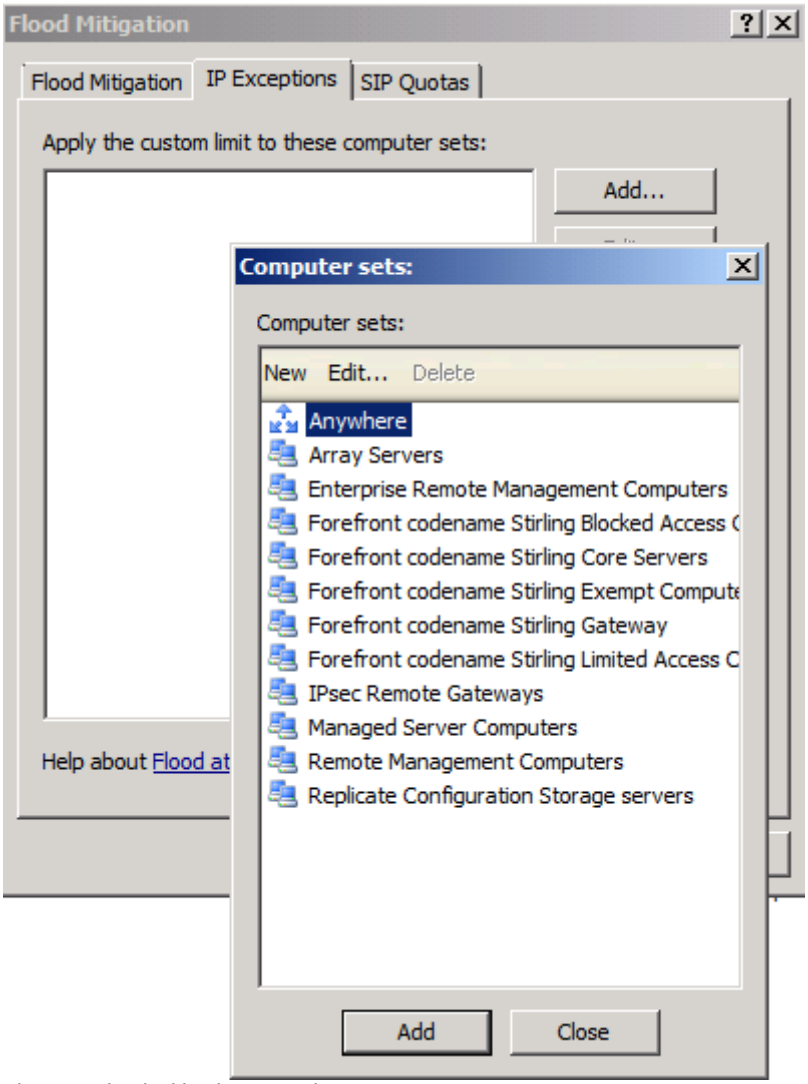

Figure 7: Flood mitigation exceptions

There are some settings like connection limits for TCP half-open connections for which you can't configure custom exceptions.

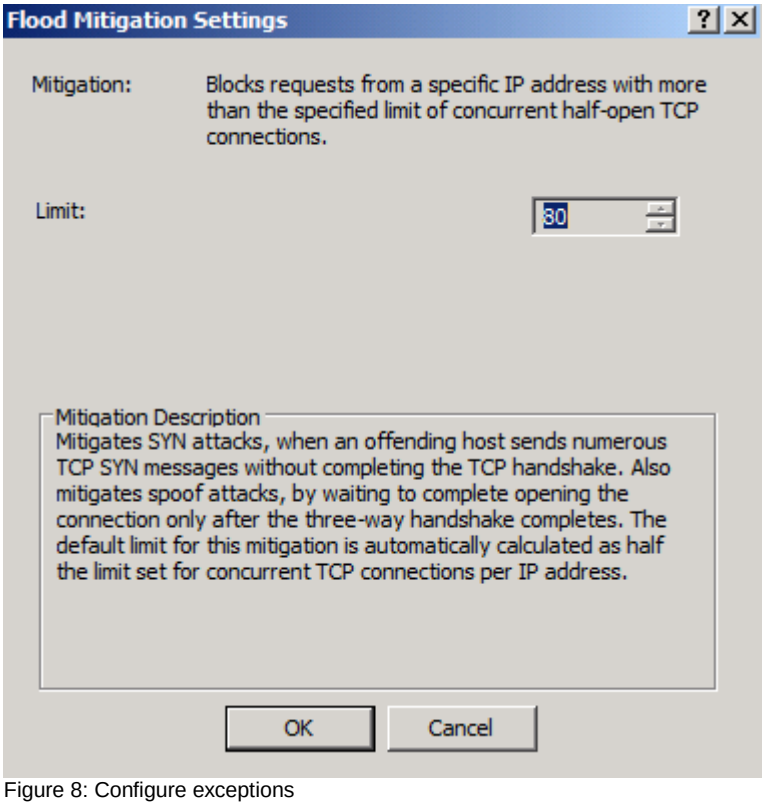

Figure 8: Configure exceptions

Configure alerts

As an Administrator you would like to know when a flood attack or spoofing attack occurs. TMG give you the possibility to configure alert definitions to alert you via e-mail, event log and many more. To configure alerts start the TMG management console, navigate to the Monitoring node and select the Alerts tab and in the task pane click Configure *Alert Definitions*.

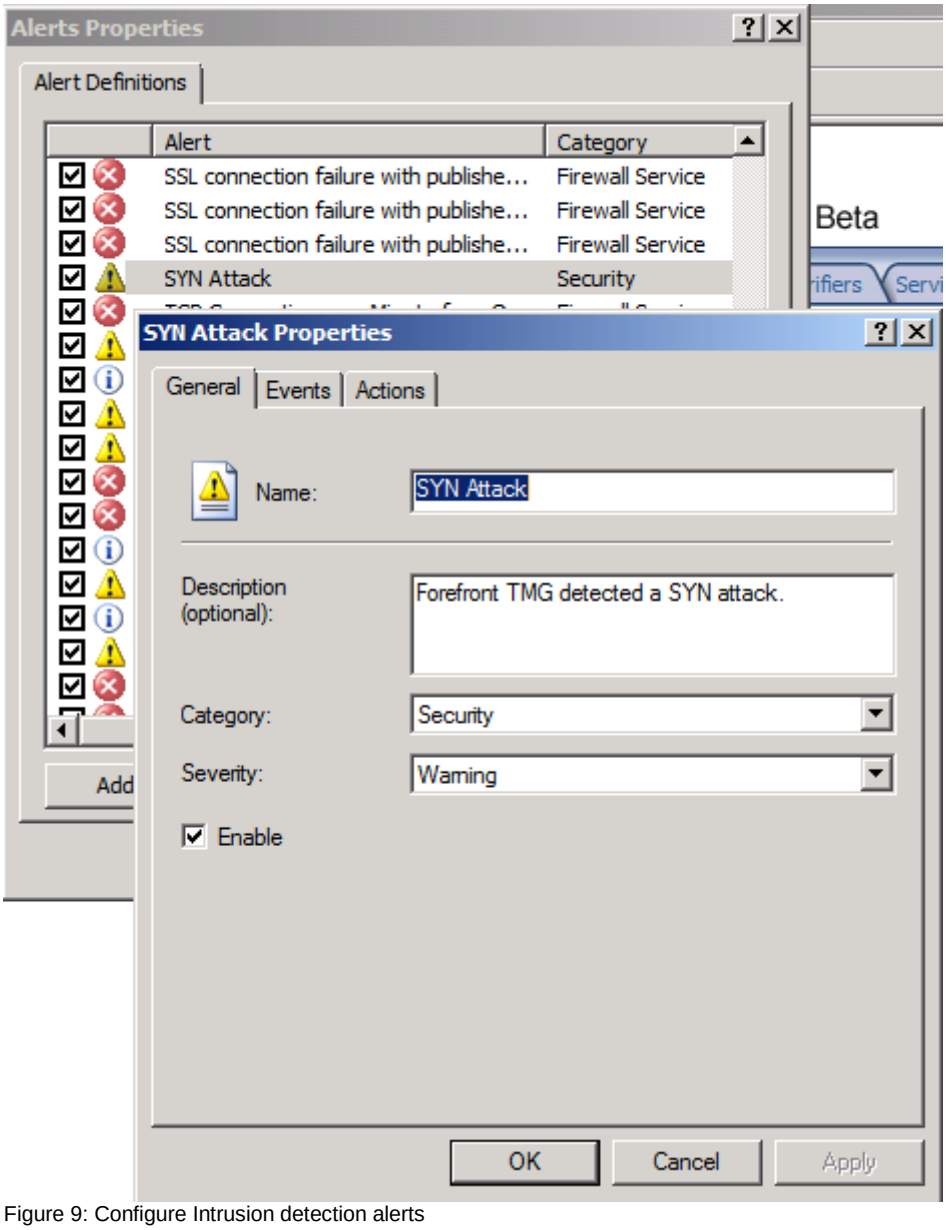

Figure 9: Configure Intrusion detection alerts

SIP Quotas

SIP (Session Initiation Protocol) support is a new feature in Microsoft Forefront TMG, but in Beta 3 of TMG with some limitations. If you plan to use this feature, you should read the Beta 3 release notes. SIP is used to provide IP based telephony services and VoIP gateways. Until ISA Server 2006 there was no support for SIP so you had to manually configure all required ports for SIP communication. Microsoft Forefront TMG comes with a builtin SIP-Filter. SIP uses SIP Quotas for its operation and Microsoft Forefront TMG allows the configuration of SIP Quota limits as you can see in the following screenshot. If you decide to configure SIP Quotas in TMG you should be carefully read the requirements of the SIP Hardware and Software vendors which settings they recommend.

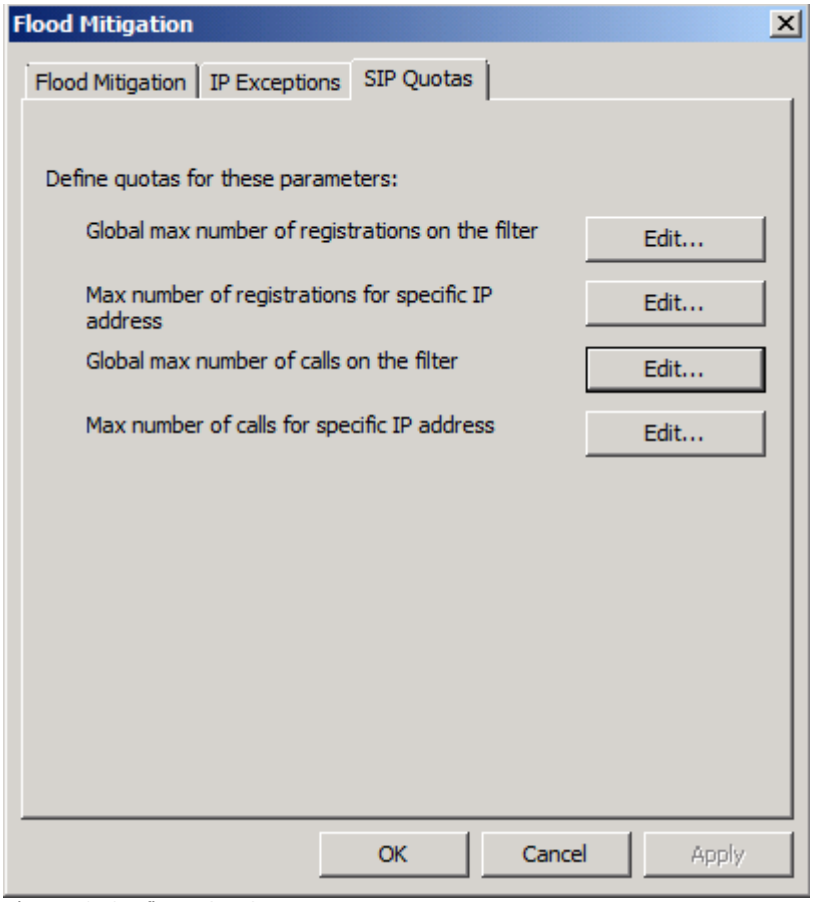

Figure 10: Configure SIP Quotas

Conclusion

In this article, I tried to show you how to configure Microsoft Forefront TMG to protect against known intrusion detection attempts and how to configure alert settings to get informed when an Intrusion on Microsoft Forefront TMG occurs.

Related links

Forefront Threat Management Gateway Beta 3
http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&displaylang=en
Forefront TMG Beta 3 is released
http://blogs.technet.com/isablog/archive/2009/06/09/forefront-tmg-beta-3-is-released.aspx
What's new in Forefront TMG Beta 2 (Part 1)
http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html
Installing and configuring Microsoft Forefront TMG Beta 2
http://www.isaserver.org/tutorials/Installing-configuring-Microsoft-Forefront-TMG-Beta2.html
Explaining and configuring NIS (Network Inspection Service)
http://www.isaserver.org/tutorials/Explaining-configuring-NIS-Network-Inspection-Service.html
ISA Server 2006 Flood Mitigation
http://www.isaserver.org/tutorials/ISA-Server-2006-Flood-Mitigation.html
Windows 7 and Windows Server 2008 R2 DirectAccess Executive Overview

http://www.microsoft.com/downloads/details.aspx?familyid=d8eb248b-8bf7-4798-a1d1-04d37f2e013c&displaylang=en