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

ISA Server 2006 Flood Mitigation

Abstract

In this article, I will show you how ISA Server 2006 provides some techniques to fight against different parts of attacks like SYN flooding, worms and unexpected large number of TCP and/or UDP connections. ISA Server 2006 calls this feature Flood Mitigation. This article will explain how to configure ISA Server Flood Mitigation.

Let's begin

Beginning with ISA Server 2000, Microsoft implemented some rudimentary Anti spoofing and intrusion detection features. ISA Server 2004 introduced some more features to fight against intrusion detection attacks. ISA Server 2006 adds additionally techniques to fight against SPAM. New technologies included are the Flood Mitigation settings that should help to protect against some additional threats. This article is focused on the Flood mitigation settings in ISA Server 2006.

Threats and countermeasures

There are different threats in our computer world. Some of these treats and feature from ISA Server 2006 to fight against these threats are:

Threat	Feature
Worms that flow from user to user and network to network to hurt users	IP alert spoofing Connection Quotas Enhanced Flood Protection Intrusion Detecion Protection against Denial of Service (DoS) and Distributed Denial of Service attacks
An increasing number of attacks on externally facing resources	Possible attacks through DHCP poisioning, Intrusion Detection and IP Fragmentation can be configured easily, to protect the corporate network
Protection against IP spoofing attacks	IP spoofing protection in ISA Server 2006. ISA Server 2006 protects against IP spoofing by checking the validity of the source IP address in the packet

Table 1: Threats and features

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 fullfill 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

Table 2: Type of Attacks

Configuring Attack Mitigation Features

ISA Server 2006 includes some attack mitigation features which you can configure and monitor with the ISA Server 2006 management console. ISA Server 2006 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 poisioning 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 ISA Server 2006 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 ISA Server 2006 helps to ensure that ISA Server can continue to function, even when is ISA under a flood attack.

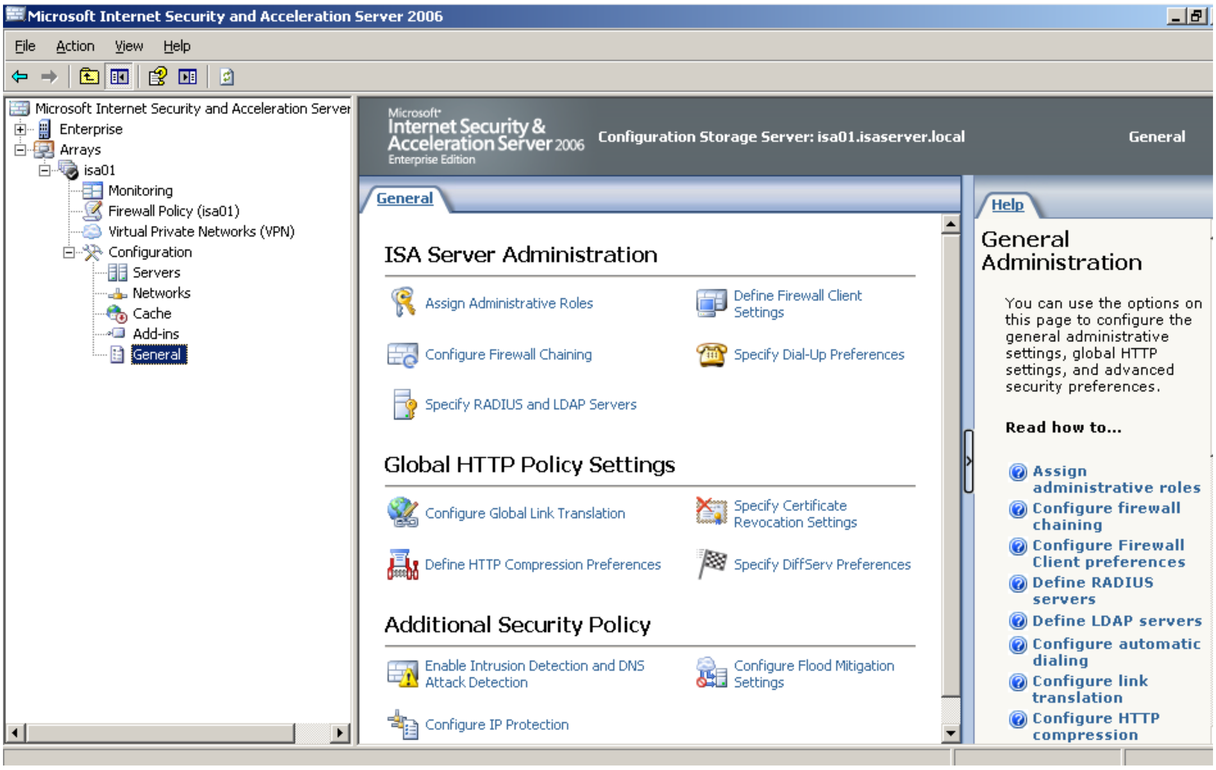
Attack	ISA Mitigation	Defaults
Flood attack. A specific IP address tries to open many connections to many different IP addresses to create a flood attack	TCP connect requests per minute, per IP address	By default, ISA Server limits the number of TCP requests per client to 600 per minute. Keep in mind 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	Concurent TCP connections üer IP address	ISA Server limits the number of TCP concurrent connections per client to 160
SYN attack. A malicipus client tries to flood ISA Srever 2006 with a large amount of half-open TCP connections	ISA Server mitigates SYN attacks.	ISA Server 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 attackcurrent UDP	UDP concurrent sessions per IP address. When a UDP flood attack occurs, ISA Server closes older sessions, so that no more than the specified number of connections is allowed concurrently	ISA Server limits the number of concurrent UDP sessions per IP address to 160. This limit is configurable to 400 concurrent UDP sessions

Table 3: ISA protection

Flood attack configuration

Let’s start with some basic steps to configure Flood Mitigation in the ISA Server 2006 Management console.

All of ISA Servers flood mitigation features and some other techniques against DNS attacks can be found under the *Configuration* - *General* node in ISA Server 2006.



Microsoft Internet Security and Acceleration Server 2006

File Action View Help

- Microsoft Internet Security and Acceleration Server
  - Enterprise
  - Arrays
    - isa01
      - Monitoring
      - Firewall Policy (isa01)
      - Virtual Private Networks (VPN)
      - Configuration
        - Servers
        - Networks
        - Cache
        - Add-ins
        - General

Microsoft® Internet Security & Acceleration Server 2006 Enterprise Edition

Configuration Storage Server: isa01.isaserver.local

General

General

ISA Server Administration

- Assign Administrative Roles
- Define Firewall Client Settings
- Configure Firewall Chaining
- Specify Dial-Up Preferences
- Specify RADIUS and LDAP Servers

Global HTTP Policy Settings

- Configure Global Link Translation
- Specify Certificate Revocation Settings
- Define HTTP Compression Preferences
- Specify DiffServ Preferences

Additional Security Policy

- Enable Intrusion Detection and DNS Attack Detection
- Configure Flood Mitigation Settings
- Configure IP Protection

Help

General Administration

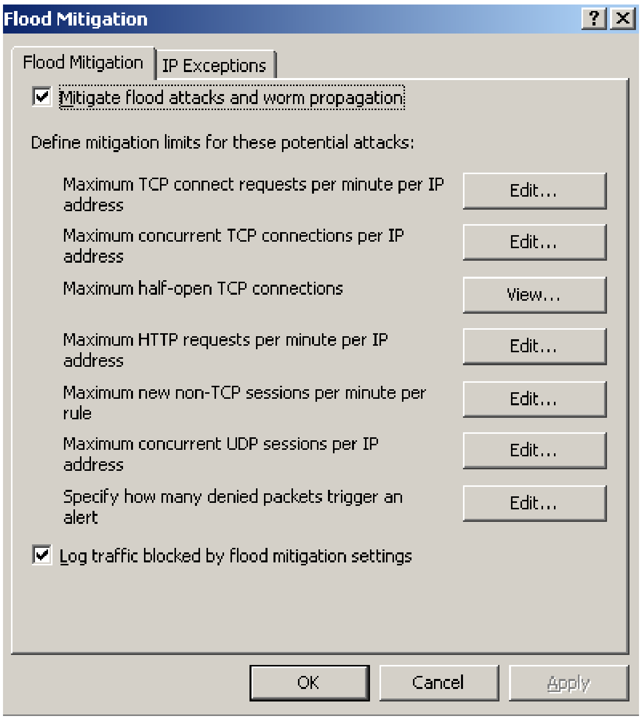
You can use the options on this page to configure the general administrative settings, global HTTP settings, and advanced security preferences.

Read how to...

- Assign administrative roles
- Configure firewall chaining
- Configure Firewall Client preferences
- Define RADIUS servers
- Define LDAP servers
- Configure automatic dialing
- Configure link translation
- Configure HTTP compression

Figure 1: ISA Server Additional Security Policy

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.



Flood Mitigation

Flood Mitigation | IP Exceptions

☑ Mitigate flood attacks and worm propagation

Define mitigation limits for these potential attacks:

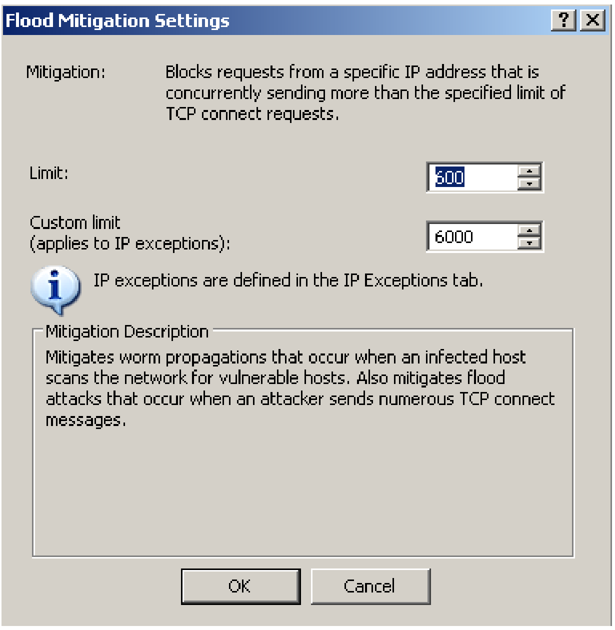
Maximum TCP connect requests per minute per IP address	Edit...
Maximum concurrent TCP connections per IP address	Edit...
Maximum half-open TCP connections	View...
Maximum HTTP requests per minute per IP address	Edit...
Maximum new non-TCP sessions per minute per rule	Edit...
Maximum concurrent UDP sessions per IP address	Edit...
Specify how many denied packets trigger an alert	Edit...

☑ Log traffic blocked by flood mitigation settings

OK Cancel Apply

Figure 2: General flood mitigation settings

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.



Mitigation: Blocks requests from a specific IP address that is concurrently sending more than the specified limit of TCP connect requests.

Limit: 600

Custom limit (applies to IP exceptions): 6000

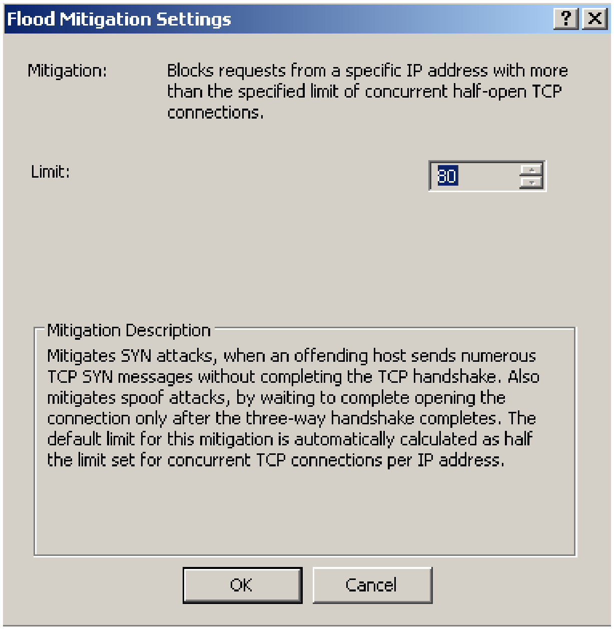
IP exceptions are defined in the IP Exceptions tab.

Mitigation Description

Mitigates worm propagations that occur when an infected host scans the network for vulnerable hosts. Also mitigates flood attacks that occur when an attacker sends numerous TCP connect messages.

Figure 3: Custopm limits for IP exceptions

There are some settings like connection limits for TCP half-open connections for which you can’t set any exceptions.



Mitigation: Blocks requests from a specific IP address with more than the specified limit of concurrent half-open TCP connections.

Limit: 80

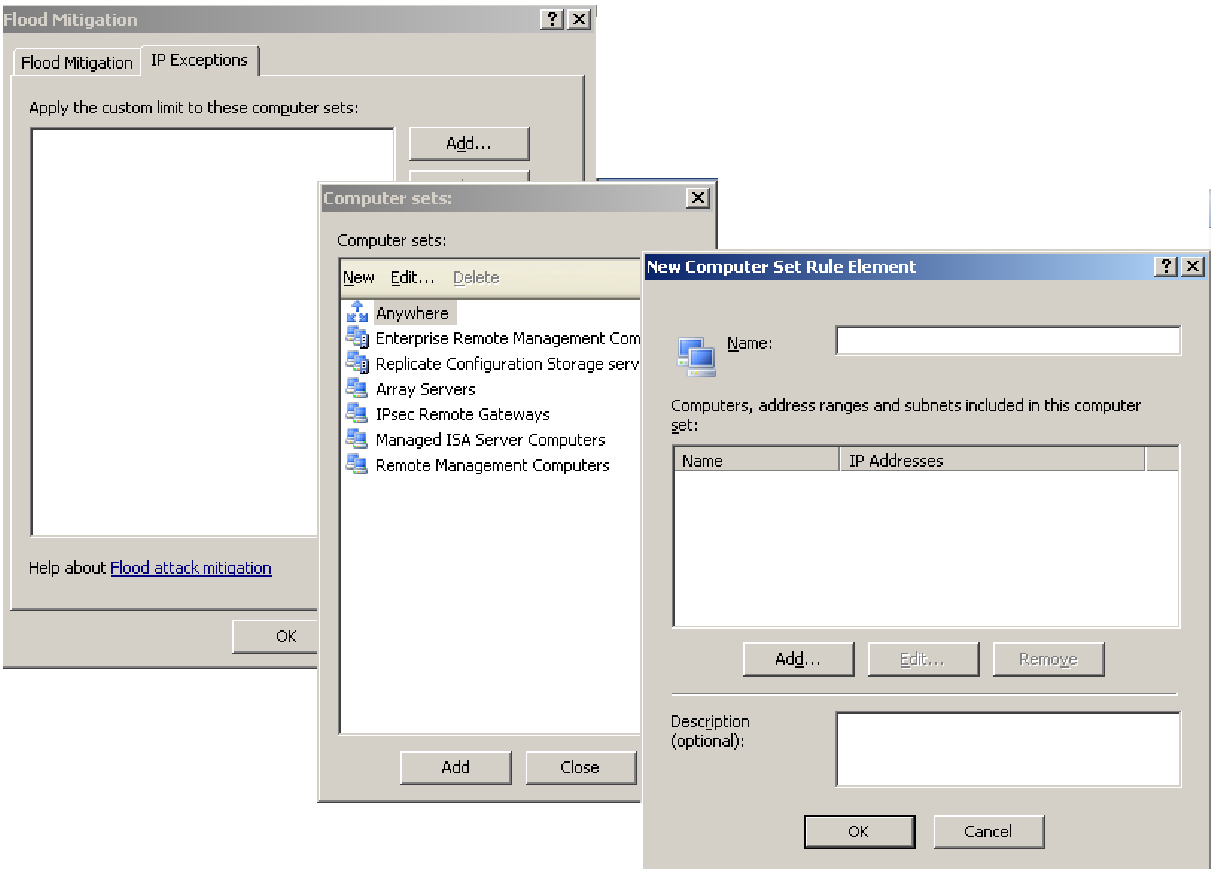
Mitigation Description

Mitigates SYN attacks, when an offending host sends numerous TCP SYN messages without completing the TCP handshake. Also mitigates spoof attacks, by waiting to complete opening the connection only after the three-way handshake completes. The default limit for this mitigation is automatically calculated as half the limit set for concurrent TCP connections per IP address.

Figure 4: Connection settings without exceptions

IP exceptions

Not every attack is an real attack from a hacker or malicious user. There are some legal reasons for clients 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 ISA server has enough resources for additional connections, it is possible to create IP exceptions as shown in the following picture.

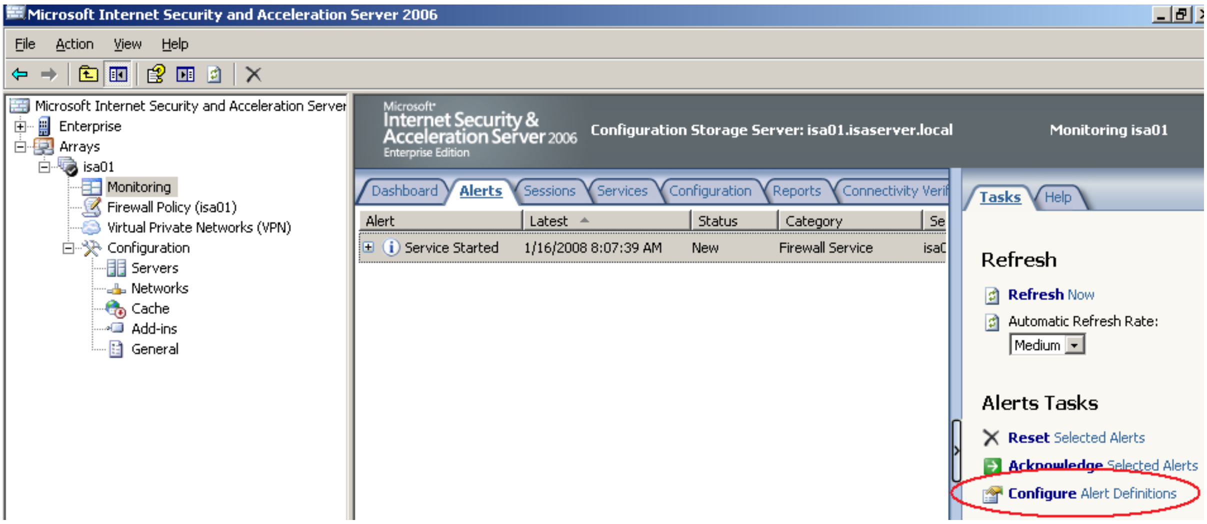

Flood Mitigation
Flood Mitigation
IP Exceptions
Apply the custom limit to these computer sets:
Add...
Help about Flood attack mitigation
OK
Computer sets:
Computer sets:
New
Edit...
Delete
Add
Close
New Computer Set Rule Element
Name:
Computers, address ranges and subnets included in this computer set:
Name
IP Addresses
Add...
Edit...
Remove
Description (optional):
OK
Cancel

- Anywhere
- Enterprise Remote Management Com
- Replicate Configuration Storage serv
- Array Servers
- IPsec Remote Gateways
- Managed ISA Server Computers
- Remote Management Computers

Figure 5: Connection settings without exceptions

Configure alerts

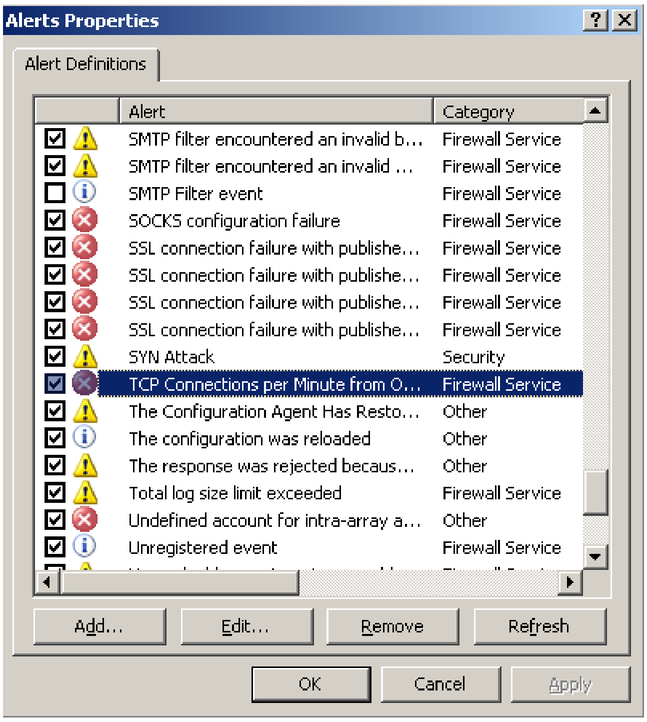
As an Administrator you would like to know when y flood attack or spoofing attack occurs. ISA Server 2006 give you the possibility to configure alert definitions to alert you via e-mail, Event log and many more.


Microsoft Internet Security and Acceleration Server 2006
File
Action
View
Help
Microsoft Internet Security and Acceleration Server
Enterprise
Arrays
isa01
Monitoring
Firewall Policy (isa01)
Virtual Private Networks (VPN)
Configuration
Servers
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2006 Enterprise Edition
Configuration Storage Server: isa01.isaserver.local
Monitoring isa01
Dashboard
Alerts
Sessions
Services
Configuration
Reports
Connectivity Verif
Tasks
Help
Refresh
Refresh Now
Automatic Refresh Rate:
Medium
Alerts Tasks
Reset Selected Alerts
Acknowledge Selected Alerts
Configure Alert Definitions

Alert	Latest	Status	Category	Se
Service Started	1/16/2008 8:07:39 AM	New	Firewall Service	isa0

Figure 6: Configure alert definitions

It is possible to create a notification for several alerts like SYN attacks and over limit connections per second or per IP address.



		Alert	Category
☑	⚠	SMTP filter encountered an invalid b...	Firewall Service
☑	⚠	SMTP filter encountered an invalid ...	Firewall Service
☐	ⓘ	SMTP Filter event	Firewall Service
☑	✖	SOCKS configuration failure	Firewall Service
☑	✖	SSL connection failure with publishe...	Firewall Service
☑	✖	SSL connection failure with publishe...	Firewall Service
☑	✖	SSL connection failure with publishe...	Firewall Service
☑	✖	SSL connection failure with publishe...	Firewall Service
☑	⚠	SYN Attack	Security
☑	✖	TCP Connections per Minute from O...	Firewall Service
☑	⚠	The Configuration Agent Has Resto...	Other
☑	ⓘ	The configuration was reloaded	Other
☑	⚠	The response was rejected becaus...	Other
☑	⚠	Total log size limit exceeded	Firewall Service
☑	✖	Undefined account for intra-array a...	Other
☑	ⓘ	Unregistered event	Firewall Service

Figure 7: Configure alert definitions for high TCP connections per minute

Logging Flood Manipulation

ISA Server 2006 is logging Flood manipulation attempts, as you can see in the following table. The table is copied from the ISA Server 2006 article about flood mitigation.

Result code	Hex ID	Details
WSA_RWS_QUOTA	0x80074E23	A connection was refused because a quota was exceeded.
FWX_E_RULE_QUOTA_EXCEEDED_DROPPED	0xC0040033	A connection was rejected because the maximum number of connections created per second for this rule was exceeded.
FWX_E_TCP_RATE_QUOTA_EXCEEDED_DROPPED	0xC0040037	A connection was rejected because the maximum connections rate for a single client host was exceeded.
FWX_E_DNS_QUOTA_EXCEEDED	0xC0040035	A DNS query could not be performed because the query limit was reached.

Table 4: ISA Flood Mitigation logging (Source: http://www.microsoft.com/technet/isa/2006/flood_resiliency.mspx)

Conclusion

Microsoft ISA Server 2006 introduces a new feature called Flood Mitigation. With the help of Flood Mitigation you can limit the number of current TCP and UDP sessions.

This can help to limit the effects of attacks to ISA Server like SYN attacks, worm attacks and many more known attacks.

Related links

ISA Firewall Flood Mitigation Settings
http://blogs.isaserver.org/shinder/2006/11/18/isa-firewall-flood-mitigation-settings/
ISA Server 2006 as a Kitchen Utensil: Part 2 - Internal Attacks
http://www.isaserver.org/tutorials/ISA-Server-2006-Kitchen-Utensil-Part2.html
Configure flood mitigation
http://technet.microsoft.com/en-us/library/bb838988.aspx
ISA Server 2006 Overview
http://www.isaserver.org/articles/isa-server-2006-overview.html
ISA Server Network Protection: Protecting Against Floods and Attacks
http://www.microsoft.com/technet/isa/2006/flood_resiliency.mspx