

DotNet Internals



Web Traffic Control

Technical documentation

Contents

Contents.....	2
Introduction	3
Pre-Requisites.....	4
How it works.....	5
How it works – continued	6
How it works – continued	7
WTC end user interface	8
WTC Zone Concept.....	9
Configuring WTC.....	10
Configure WTC – Database Settings	11
Configure WTC – General WTC Settings.....	12
Configure WTC – Configure WTC Zones (Array)	13
Configure WTC – Configure WTC Zones (Zones).....	14
Configure WTC – Configure WTC Zones (Zones).....	15
Configure WTC – Configure WTC Zones (Zones).....	16
Adding WTC Sharepoint Pages	17

Introduction

Web Traffic Control (WTC) is a product that let's end users easily control internet access for their users. The product is built on top of Microsoft ISA Server 2006 and is hosted through Sharepoint Portal Server 2007.

This guide will describe the solution as an wtc administrator and a wtc end-user.

Basic functions:

- Block a pc by its name
- Block groups of pc's or a classroom
- Block users from active directory
- Block groups from active directory
- On-Demand Update (access is blocked instantly)

Advanced functions:

- Add URL exception
- Add domain exception
- Choose the active time for when users should be blocked (10:30-11:00)
- Choose what protocols to block (MSN, or other custom protocols)

Pre-Requisites

- Microsoft ISA Server 2006 (Enterprise)
- Microsoft Office Sharepoint Server 2007
- Microsoft .Net Framework 3.5 SP1
- Microsoft SQL Server 2005 and up
- Sliverlight 3 (on the clients)
- No software installation required on the client PC's

Note! We recommend setting up a separate ISA Server that's purpose is only for WTC rules.

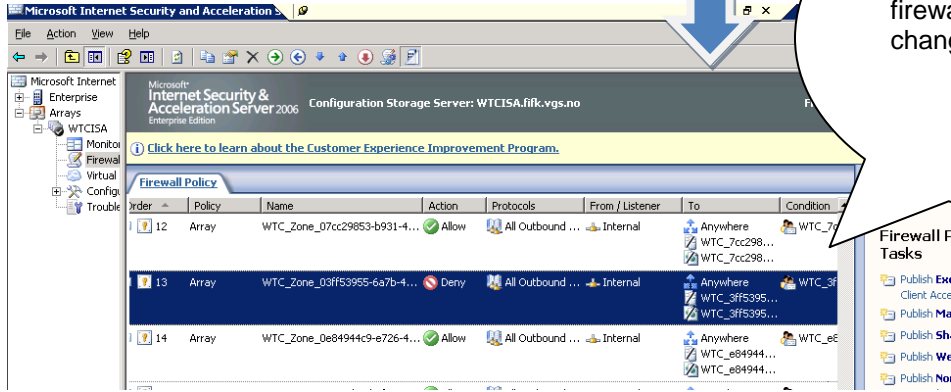
How it works

User sets a start & end time.
Selects what users/groups to control.
Adds exception domains or url's,
www.bbc.com or
www.bbc.com/page.htm

User selects the WTC zone that fits their needs. E.g. All Closed, All Open, Exam, etc.



WTC communicates with ISA server and makes sure the firewall array reflects the changes the end user did



How it works – continued

WTC is based on the following technologies.

Silverlight:

- Contains the end-user interface for interacting with WTC zones

Sharepoint:

- Sharepoint is the main UI for administrators of WTC.
- Create/modify/delete WTC zones
- Distribute WTC zones to end users through Sharepoint web part pages
- Regular Sharepoint access control is used to decide what users have control over what zones

ISA Server:

- WTC zone definitions convert into ISA firewall rules.
- ISA administrator can extend or modify parts of the WTC firewall rule

How it works – continued

WTC relies on ISA server to do the actual blocking of users, groups and computers. The clients that are to be controlled by specifying user or group needs to be configured as web-proxy clients. We recommend configuring the clients with WPAD settings of the DHCP scope. WPAD will allow you to set the configuration of Internet Explorer on the clients only when they are connected to a specific subnet. So if the user brings the computer to another location or home the settings will be removed.

WTC end user interface



Displays the name of the WTC Zone

Displays the name of the logged on user

Start and end time for when the zone is active.

Add exception url's directly to specific internet domains. E.g. www.facebook.com to allow all content in facebook.

Add exception url's directly to specific internet pages.

Add users/groups or computers

Remove selected users/groups or computers

Updates ISA Server

WTC Zone Concept

WTC has support for three zone types. WTC zones will convert into ISA server firewall rules. A WTC zone can support computers & groups of computers, users and groups (AD) or both. Keep in mind that supporting both will create two firewall rules per zone instead of one.

Personal WTC Zone

A personal zone will let each user of WTC have their own settings, list of members, url and domain exception lists. This will require one or two firewall rules per user.

Shared WTC Zone

A shared zone will let multiple users access the same settings, list of members, url and domain exception lists. This will require one or two firewall rules per zone.

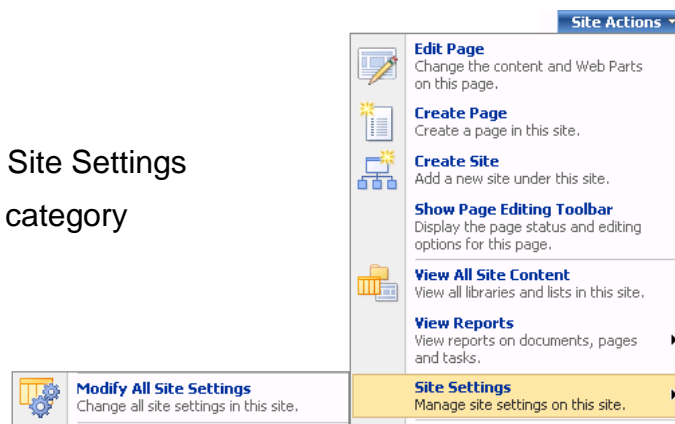
Isolated member Zone

A isolated member zone will let multiple users share the same url and domain exception lists, but the list of members will be personal. This is the recommended zone type for larger installations.

Configuring WTC

To access the WTC settings:

1. Site Actions > Site Settings > Modify All Site Settings
2. Locate the Web Traffic Control Settings category



Web Traffic Control Settings

- [Configure WTC Zones](#)
- [Configure General WTC Settings](#)
- [Configure Database Settings](#)

Configure WTC – Database Settings

Click the configure Database Settings link in the Web Traffic Control Settings category of site settings.

This dialog will let you create the WTC database that should be used.

1. Type in the SQL connection string that points to the SQL server you want to use for WTC.
2. Select the use supplied credentials and type in the user credentials for a user that has sysadmin permissions on the SQL Server
3. Push the “Create and Save Config” button

Web Traffic Control 2008 - Database Settings

Admin page for creating or modifying the WTC database

License: Finmark fylkeskommune

WTC Connectionstring
Please type in a descriptive name and description for the WTC zone.

SQL ConnectionString
Data Source=WTCSHPV\OFFICESERVERS;Initial Catalog=WebTra

Use External Credentials
If your current logged on user account does not have permissions to create a new database you can supply your own. This might also be necessary if the database is located on another physical server.

Use supplied credentials
 Use supplied credentials

USERNAME
DOMAIN
PASSWORD

Errors and messages

Save Configuration Test Connectionstring Create and Save Config Cancel

Configure WTC – General WTC Settings

The configure general WTC settings page lets you set up the connection to the ISA server.

Active Directory LDAP

E.g. dc=domain,dc=com

Active Directory server FQDN

E.g. domain.com

ISA Server Name or IP

E.g. isa.domain.com or xxx.xxx.xxx.xxx

ISA WTC Service Port

Should be 9000

ISA WTC User Principal Logon Name

Same name as the user running the WTC windows service on the ISA Server.

Web Traffic Control 2008 - General Settings

Admin page for modifying general settings

License: Finmark fylkeskommune

Active Directory Information
Please type in distinguishedname of the root element you want to use in active directory.

Active Directory LDAP
dc=fifk,dc=vgs,dc=no

Active Directory Server FQDN
fifk.vgs.no

ISA Server Configuration
If your current logged on user account does not have permissions to create a new database you can supply your own. This might also be necessary if the database is located on another physical server.

ISA Server Name or IP
172.20.1.22

ISA WTC Service Port
9000

ISA WTC User Principal Logon Name
WTCService@fifk.vgs.no

Save Configuration Cancel

Configure WTC – Configure WTC Zones (Array)

Selecting and configuring ISA arrays.
Click the ISA array you want to include

Web Traffic Control Linked ISA Arrays	
Before you can start to create your zones you need to enable the ISA arrays you want to make available for WTC.	
Name	Enabled
WTCISA	<input checked="" type="checkbox"/>

Select the “Allow WTC to use this array” checkbox.



Select what protocols WTC should be able to expose for the user.

If any address ranges are defined on the ISA server then select the one's you want to include in the WTC zones.

Click the Save Array button

WTC ISA Array In this section you can choose if this ISA array will be available for Web Traffic Control zones.	General Settings <input checked="" type="checkbox"/> Allow WTC to use this array
ISA Schedules Select what schedules you want to make available from this ISA Array.	Select ISA Schedules <input type="checkbox"/> Weekends <input type="checkbox"/> Work hours
ISA Applications Select what applications you want to make available to WTC from this Array.	Select ISA Applications <input type="checkbox"/> AOL Instant Messenger <input type="checkbox"/> Archie <input type="checkbox"/> Chargen (TCP) <input type="checkbox"/> Chargen (UDP) <input type="checkbox"/> Daytime (TCP) <input type="checkbox"/> Daytime (UDP) <input type="checkbox"/> DHCP (reply) <input type="checkbox"/> DHCP (request)
ISA Address Ranges Select what Address Ranges you want to make available to WTC from this Array.	Select ISA Address Ranges

Configure WTC – Configure WTC Zones (Zones)

Click the create new WTC zone link to create a new WTC zone or click one of the existing WTC zones to modify.

The administrator can get a list of all the blocked users, and they can add permanent urls and domains for the zone.

Web Traffic Control Zones

This is an overview of all the zones defined in Web Traffic Control. These zones can be linked into web parts organized around your sharepoint structure

Name	Connected ISA Array	Enabled
Hammerfest vgs - ingen sosiale medier view blocked users add permanent urls and domains	WTCISA	✓
Vadsø vgs - kun PAS og PGS view blocked users add permanent urls and domains	WTCISA	✓

[Create new WTC Zone](#)

[Go back to settings](#)

Web Traffic Control Zone Permanent Urls

This is an overview of all the permanent urls for this zone

Action	Url	Added By
Delete	blink.dagbladet.no	admpest

URL

Web Traffic Control Zone Permanent Domains

This is an overview of all the permanent domains for this zone

Action	Domain	AddedBy
Delete	biip.no	admpest
Delete	flickr.com	admpest
Delete	netlog.com	admpest
Delete	facebook.com	admpest
Delete	myspace.com	admpest
Delete	secondlife.com	admpest
Delete	spill.no	admpest
Delete	twitter.com	admpest

Domain

Configure WTC – Configure WTC Zones (Zones)

Zone Name:

Add a descriptive name that's unique for the zone. The end-user will see this name.

Included Elements:

Select what types of objects the zone can include. Computer, users or both.

Rule Type:

A zone can be set to default deny or default allow. A zone that is configured to deny will allow the url and domains added to the exception list.

WTC Zone Type:

Select the zone type

ISA Array

Select what ISA array this zone should be stored in.

Active Directory – User:

Specify ldap root and search filter for what users this zone can contain.

Web Traffic Control 2008 - Zone Settings

Admin page for configuring zone settings

License: Finmark fylkeskommune

WTC Name and Description
Please type in a descriptive name and description for the WTC zone.

Zone Name

Zone Description

Include Elements
In this section you can control what elements the zone can contain. E.g. Users, Groups, Computers or Address Ranges

Included Elements
 User & Group Objects
 Computer & ISA Address Range Objects

Rule Type
In this section you can control if the zone type should allow all traffic except what is specified or if it should deny all except what is specified

Select Rule Type
 Default Deny
 Default Allow

Zone Type
There are three different WTC zone types you can choose amongst. Personal Zone: Lets a specific user modify members, and details of the zone. Shared Zone: More than one user can modify this type of zone, they will share the list of members and all other settings. Isolated Member Zone: This type of zone the users will get their own member list and they only share the settings for the zone.

Select WTC Zone Type
 Personal WTC Zone
 Shared WTC Zone
 Isolated Member Zone

ISA Array
A WTC zone will be connected to a specific ISA array. You can make Schedules, applications and address ranges available to the zone with the checkboxes.

Select ISA Array

Select ISA Applications

Active Directory - User
It is important to limit what users can be selected in a scope. You have to specify a search root for users, groups and computers and you also need to specify ldap filters for what users that can be fetched. This increases the security and gives you more control.

Specify LDAP root for user search

Specify LDAP filter for user search

Configure WTC – Configure WTC Zones (Zones)

Active Directory – Group:

Specify ldap root and search filter for what groups this zone can contain.

Active Directory – Computer:

Specify ldap root and search filter for what computers this zone can contain.

Active Directory - Group

It is important to limit what users can be selected in a scope. You have to specify a search root for users, groups and computers and you also need to specify ldap filters for what users that can be fetched. This increases the security and gives you more control.

Active Directory - Computer

It is important to limit what users can be selected in a scope. You have to specify a search root for users, groups and computers and you also need to specify ldap filters for what users that can be fetched. This increases the security and gives you more control.

Specify LDAP root for group search

LDAP://ou=Auto Grupper,ou=HFEST,ou=Skoler,dc=fifk,dc=vgs,c

Specify LDAP filter for group search

(&(&(objectCategory=group)(objectSid=*)(ObjectClass=group))

Specify LDAP root for computer search

LDAP://ou=HFEST,ou=Skoler,dc=fifk,dc=vgs,dc=no

Specify LDAP filter for computer search

(&(&(objectCategory=computer)(objectSid=*)(ObjectClass=com

Save Zone

Delete Zone

Cancel

Adding WTC Sharepoint Pages

After you have configured WTC zones you need to create sharepoint pages that contain the WTC web part.

To add the WTC web part, add a new web part page and then click add new web part.

Select the Web Traffic Control 2008 web part

Edit the Web Part Settings and connect the web part with a wtc zone.

Note!

You should also set the width and height as shown in the picture to the right.

