Tweaking the configuration of Forefront TMG with customized TMG XML configuration files

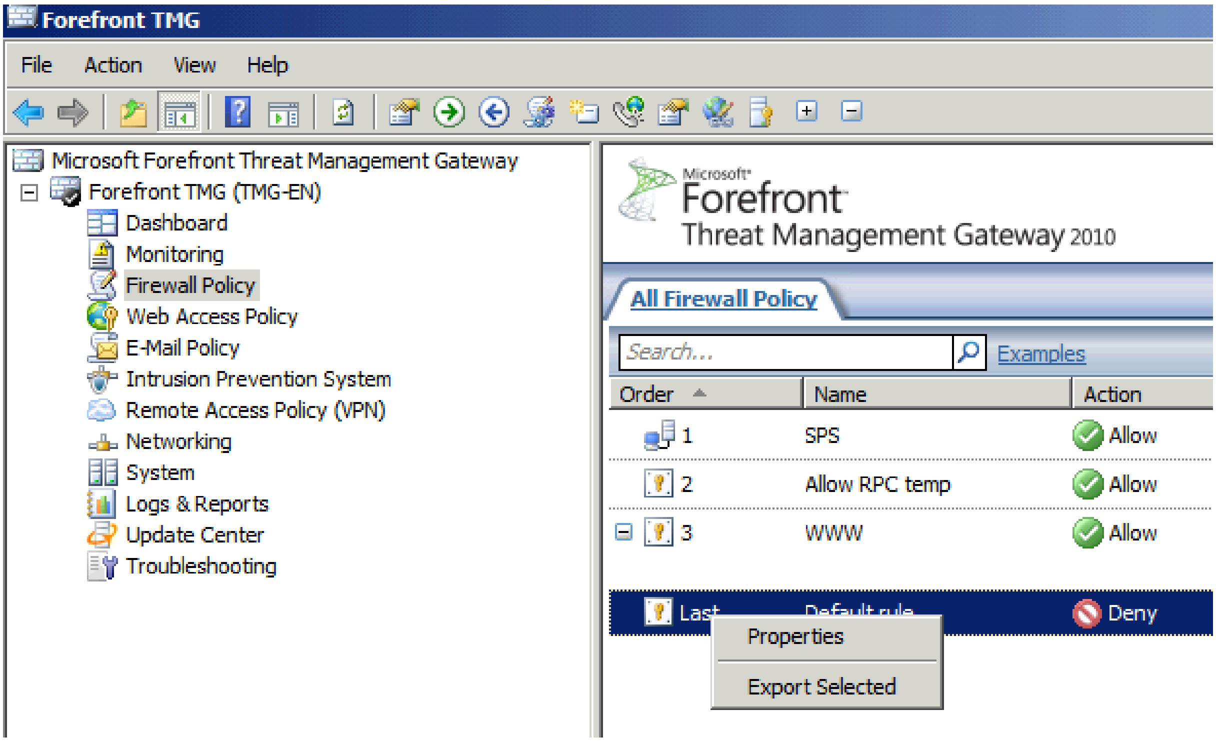
Abstract

In this article I will show you how to use the export and import functionality of Forefront TMG to tweak some TMG configuration settings which are normally not accessible or changeable in the Forefront TMG management console.

Let's begin

Before we start how to tweak the Forefront TMG configuration with modified XML export/import files I must tell you that you must use this information at your own risk, no warranty and I recommend to always create a backup of your TMG configuration before you modify something.

Forefront TMG as its predecessor ISA Server 2006 has the capability to back up the entire Forefront TMG configuration or parts of the Forefront TMG configuration into a XML file. You can use this XML files to restore the configuration on the same or a different Forefront TMG server. The following screenshot shows an example how to export a Firewall policy rule into an XML file. For more information about the backup and restore process of Forefront TMG, read the following article.

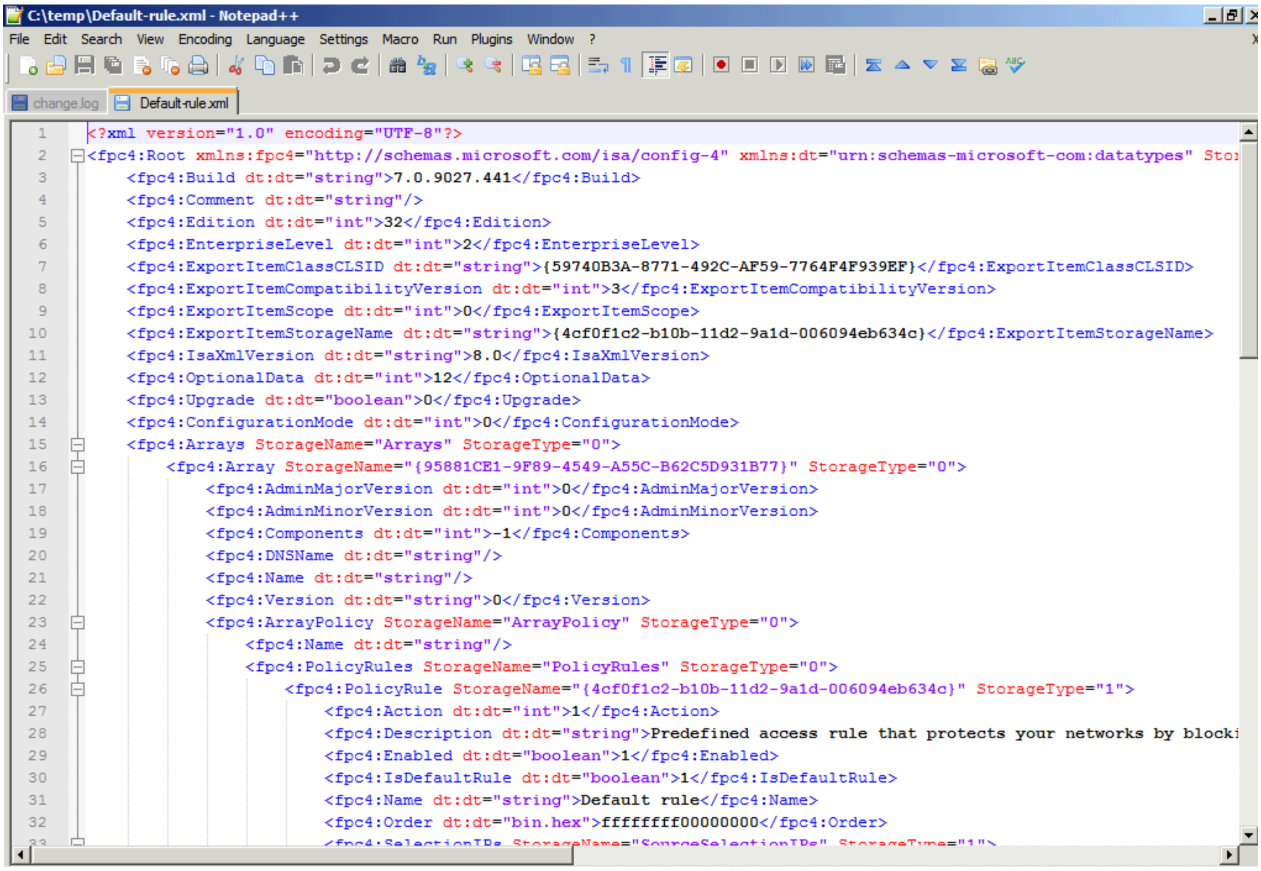


Order	Name	Action
1	SPS	Allow
2	Allow RPC temp	Allow
3	WWW	Allow
Last	Default rule	Deny

Figure 1: Export selected Firewall policy rule

Quick note: The backup and restore process backs up and restores certificate keys, which indicate to Forefront TMG which certificates to use, but it NOT backups the certificates themselves, so you always have to create a backup of your certificates on the TMG server with the import and export functionality of the certificate MMC Snap In from Windows Server 2008/R2 and you should place the certificates on a secure location because the certificate contains the private key which is used to decrypt the encrypted network traffic.

The following screenshot shows an example of an exported Firewall policy rule, in this example the Default Firewall policy rule of Forefront TMG.

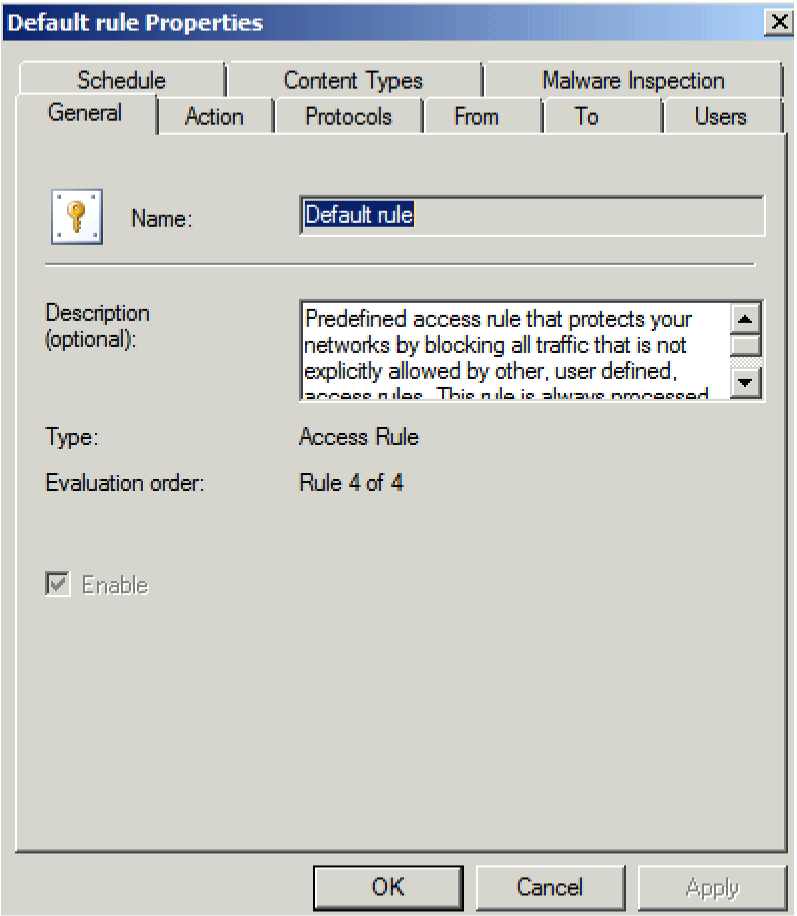

C:\temp\Default-rule.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
change.log
Default-rule.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<fpc4:Root xmlns:fpc4="http://schemas.microsoft.com/isa/config-4" xmlns:dt="urn:schemas-microsoft-com:datatypes" Sto
    <fpc4:Build dt:dt="string">7.0.9027.441</fpc4:Build>
    <fpc4:Comment dt:dt="string"/>
    <fpc4:Edition dt:dt="int">32</fpc4:Edition>
    <fpc4:EnterpriseLevel dt:dt="int">2</fpc4:EnterpriseLevel>
    <fpc4:ExportItemClassCLSID dt:dt="string">{59740B3A-8771-492C-AF59-7764F4F939EF}</fpc4:ExportItemClassCLSID>
    <fpc4:ExportItemCompatibilityVersion dt:dt="int">3</fpc4:ExportItemCompatibilityVersion>
    <fpc4:ExportItemScope dt:dt="int">0</fpc4:ExportItemScope>
    <fpc4:ExportItemStorageName dt:dt="string">{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}</fpc4:ExportItemStorageName>
    <fpc4:IsaXmlVersion dt:dt="string">8.0</fpc4:IsaXmlVersion>
    <fpc4:OptionalData dt:dt="int">12</fpc4:OptionalData>
    <fpc4:Upgrade dt:dt="boolean">0</fpc4:Upgrade>
    <fpc4:ConfigurationMode dt:dt="int">0</fpc4:ConfigurationMode>
    <fpc4:Arrays StorageName="Arrays" StorageType="0">
        <fpc4:Array StorageName="{95881CE1-9F89-4549-A55C-B62C5D931B77}" StorageType="0">
            <fpc4:AdminMajorVersion dt:dt="int">0</fpc4:AdminMajorVersion>
            <fpc4:AdminMinorVersion dt:dt="int">0</fpc4:AdminMinorVersion>
            <fpc4:Components dt:dt="int">-1</fpc4:Components>
            <fpc4:DNSName dt:dt="string"/>
            <fpc4:Name dt:dt="string"/>
            <fpc4:Version dt:dt="string">0</fpc4:Version>
            <fpc4:ArrayPolicy StorageName="ArrayPolicy" StorageType="0">
                <fpc4:Name dt:dt="string"/>
                <fpc4:PolicyRules StorageName="PolicyRules" StorageType="0">
                    <fpc4:PolicyRule StorageName="{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}" StorageType="1">
                        <fpc4:Action dt:dt="int">1</fpc4:Action>
                        <fpc4:Description dt:dt="string">Predefined access rule that protects your networks by blocki
                        <fpc4:Enabled dt:dt="boolean">1</fpc4:Enabled>
                        <fpc4:IsDefaultRule dt:dt="boolean">1</fpc4:IsDefaultRule>
                        <fpc4:Name dt:dt="string">Default rule</fpc4:Name>
                        <fpc4:Order dt:dt="bin.hex">ffffffff00000000</fpc4:Order>
                        <fpc4:SelectionIPs StorageName="SourceSelectionIPs" StorageType="1">
```

Figure 2: Edit an XML file with an XML editor

Activating and deactivating the default rule

The Default Firewall Policy rule of Forefront TMG cannot be deactivated within the Forefront TMG MMC. Under normal circumstances it should not be necessary to disable the Default Firewall Policy rule because this rule works a “catch all” rule for traffic which is not explicitly allowed or denied to the Forefront TMG System policy rules or user defined Firewall Policy rules. If you have the requirement to disable the Default Firewall Policy rule, you must export the rule and after that you must edit the rule with a text editor like Notepad.exe or better a specialized XML editor. For this article I used Notepad++ as the editor.



Name: Default rule

Description (optional): Predefined access rule that protects your networks by blocking all traffic that is not explicitly allowed by other, user defined, access rules. This rule is always processed

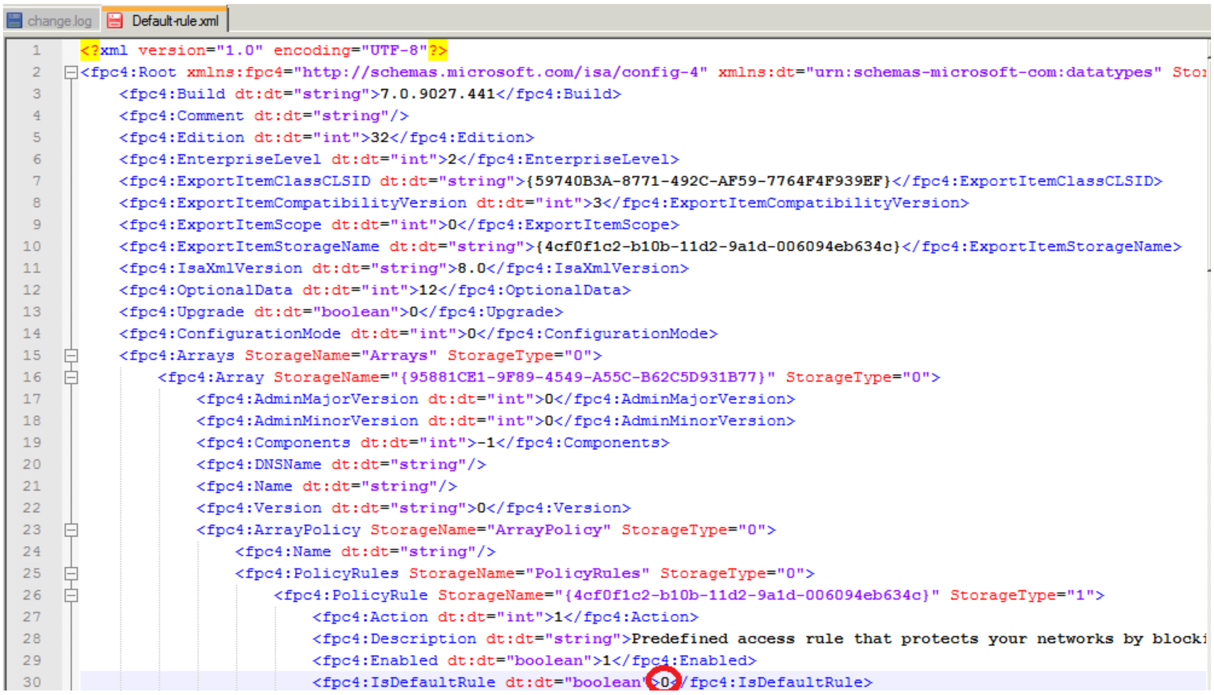
Type: Access Rule

Evaluation order: Rule 4 of 4

☑ Enable

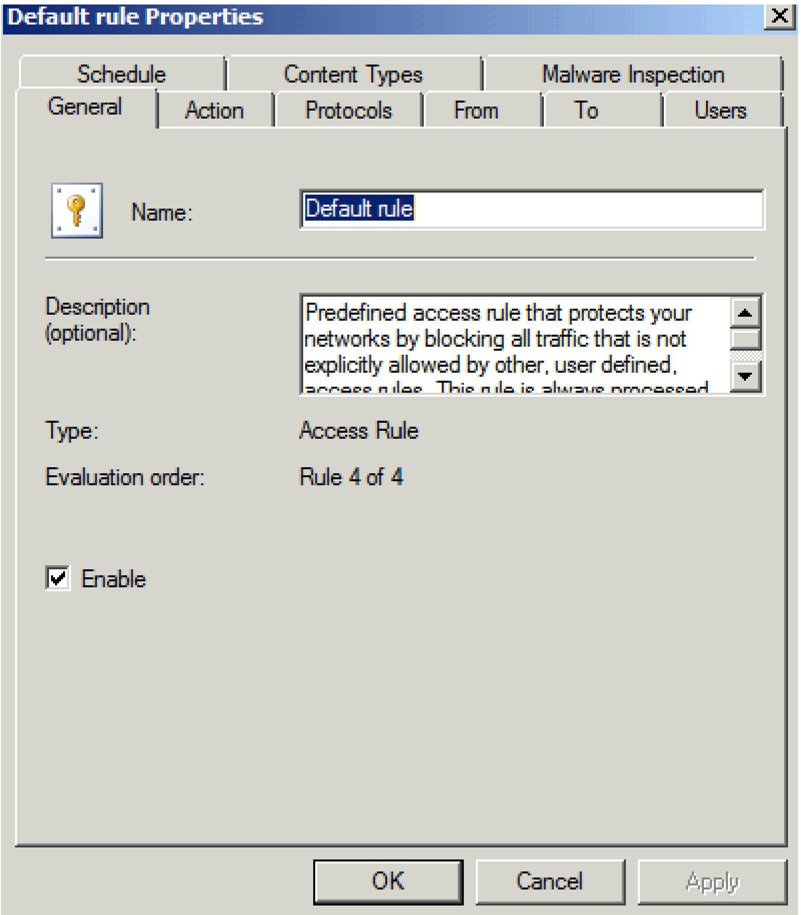
Figure 3: The default Firewall policy rule cannot be disabled

To deactivate or activate the system policy rule, export the Default Firewall Policy rule with the TMG MMC into a XML file and edit the XML file with a text or XML editor and change the “IsDefaultRule” entry to 0 from 1 and save the XML file, as shown in the following screenshot.



```
<?xml version="1.0" encoding="UTF-8"?>
<fpc4:Root xmlns:fpc4="http://schemas.microsoft.com/isa/config-4" xmlns:dt="urn:schemas-microsoft-com:datatypes" Sto
    <fpc4:Build dt:dt="string">7.0.9027.441</fpc4:Build>
    <fpc4:Comment dt:dt="string"/>
    <fpc4:Edition dt:dt="int">32</fpc4:Edition>
    <fpc4:EnterpriseLevel dt:dt="int">2</fpc4:EnterpriseLevel>
    <fpc4:ExportItemClassCLSID dt:dt="string">{59740B3A-8771-492C-AF59-7764F4F939EF}</fpc4:ExportItemClassCLSID>
    <fpc4:ExportItemCompatibilityVersion dt:dt="int">3</fpc4:ExportItemCompatibilityVersion>
    <fpc4:ExportItemScope dt:dt="int">0</fpc4:ExportItemScope>
    <fpc4:ExportItemStorageName dt:dt="string">{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}</fpc4:ExportItemStorageName>
    <fpc4:IsaXmlVersion dt:dt="string">8.0</fpc4:IsaXmlVersion>
    <fpc4:OptionalData dt:dt="int">12</fpc4:OptionalData>
    <fpc4:Upgrade dt:dt="boolean">0</fpc4:Upgrade>
    <fpc4:ConfigurationMode dt:dt="int">0</fpc4:ConfigurationMode>
    <fpc4:Arrays StorageName="Arrays" StorageType="0">
        <fpc4:Array StorageName="{95881CE1-9F89-4549-A55C-B62C5D931B77}" StorageType="0">
            <fpc4:AdminMajorVersion dt:dt="int">0</fpc4:AdminMajorVersion>
            <fpc4:AdminMinorVersion dt:dt="int">0</fpc4:AdminMinorVersion>
            <fpc4:Components dt:dt="int">-1</fpc4:Components>
            <fpc4:DNSName dt:dt="string"/>
            <fpc4:Name dt:dt="string"/>
            <fpc4:Version dt:dt="string">0</fpc4:Version>
            <fpc4:ArrayPolicy StorageName="ArrayPolicy" StorageType="0">
                <fpc4:Name dt:dt="string"/>
                <fpc4:PolicyRules StorageName="PolicyRules" StorageType="0">
                    <fpc4:PolicyRule StorageName="{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}" StorageType="1">
                        <fpc4:Action dt:dt="int">1</fpc4:Action>
                        <fpc4:Description dt:dt="string">Predefined access rule that protects your networks by blocki
                        <fpc4:Enabled dt:dt="boolean">1</fpc4:Enabled>
                        <fpc4:IsDefaultRule dt:dt="boolean">0</fpc4:IsDefaultRule>
```

After the XML file has been modified, import the XML file into your TMG configuration and from now on it is possible to activate or deactivate the default rule with the TMG MMC:



Name: Default rule

Description (optional): Predefined access rule that protects your networks by blocking all traffic that is not explicitly allowed by other, user defined, access rules. This rule is always processed

Type: Access Rule

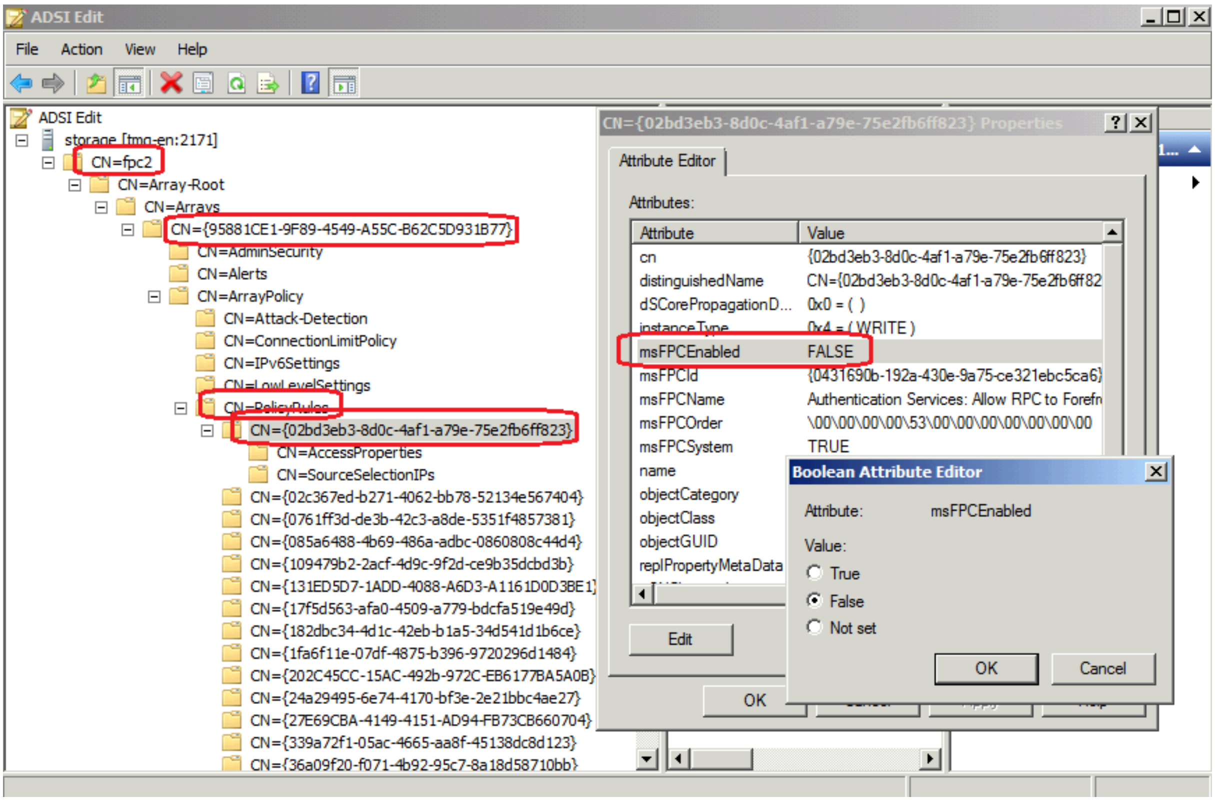
Evaluation order: Rule 4 of 4

☑ Enable

Figure 4: The default Firewall policy rule can now be activated or deactivated

Enable or disable the rule with ADSIEDIT

It is also possible to enable or disable the Firewall policy rule with ADSIEDIT. Forefront TMG stores the configuration into a AD-LDS (Active Directory Lightweight Directory Service) instance, and it is possible to edit the TMG configuration with ADSIEDIT. You can read more abot the TMG storage in the following article.
Start ADSIEDIT and connect to the TMG storage, navigate to the Firewall policy rule which you want to enable or disable and change the msFPCEnabled attribute to a value you want (true or false) as shown in the following screenshot.



```
ADSI Edit
  storage [tmg-en:2171]
    CN=fpc2
      CN=Array-Root
        CN=Arrays
          CN={95881CE1-9F89-4549-A55C-B62C5D931B77}
            CN=AdminSecurity
            CN=Alerts
            CN=ArrayPolicy
              CN=Attack-Detection
              CN=ConnectionLimitPolicy
              CN=IPv6Settings
              CN=LowLevelSettings
              CN=PolicyRules
                CN={02bd3eb3-8d0c-4af1-a79e-75e2fb6ff823}
                  CN=AccessProperties
                  CN=SourceSelectionIPs
                CN={02c367ed-b271-4062-bb78-52134e567404}
                CN={0761ff3d-de3b-42c3-a8de-5351f4857381}
                CN={085a6488-4b69-486a-adbc-0860808c44d4}
                CN={109479b2-2acf-4d9c-9f2d-ce9b35dcbd3b}
                CN={131ED5D7-1ADD-4088-A6D3-A1161D0D3BE1}
                CN={17f5d563-afa0-4509-a779-bdcfa519e49d}
                CN={182dbc34-4d1c-42eb-b1a5-34d541d1b6ce}
                CN={1fa6f11e-07df-4875-b396-9720296d1484}
                CN={202C45CC-15AC-492b-972C-EB6177BA5A0B}
                CN={24a29495-6e74-4170-bf3e-2e21bbc4ae27}
                CN={27E69CBA-4149-4151-AD94-FB73CB660704}
                CN={339a72f1-05ac-4665-aa8f-45138dc8d123}
                CN={36a09f20-f071-4b92-95c7-8a18d58710bb}
```

CN={02bd3eb3-8d0c-4af1-a79e-75e2fb6ff823} Properties

Attributes:

Attribute	Value
cn	{02bd3eb3-8d0c-4af1-a79e-75e2fb6ff823}
distinguishedName	CN={02bd3eb3-8d0c-4af1-a79e-75e2fb6ff82
dSCorePropagationD...	0x0 = ( )
instanceType	0x4 = (WRITE)
msFPCEnabled	FALSE
msFPCId	{0431690b-192a-430e-9a75-ce321ebc5ca6}
msFPCName	Authentication Services: Allow RPC to Forefr
msFPCOrder	\00\00\00\00\53\00\00\00\00\00\00\00
msFPCSystem	TRUE
name	
objectCategory	
objectClass	
objectGUID	
replPropertyMetaData	

Boolean Attribute Editor

Attribute: msFPCEnabled

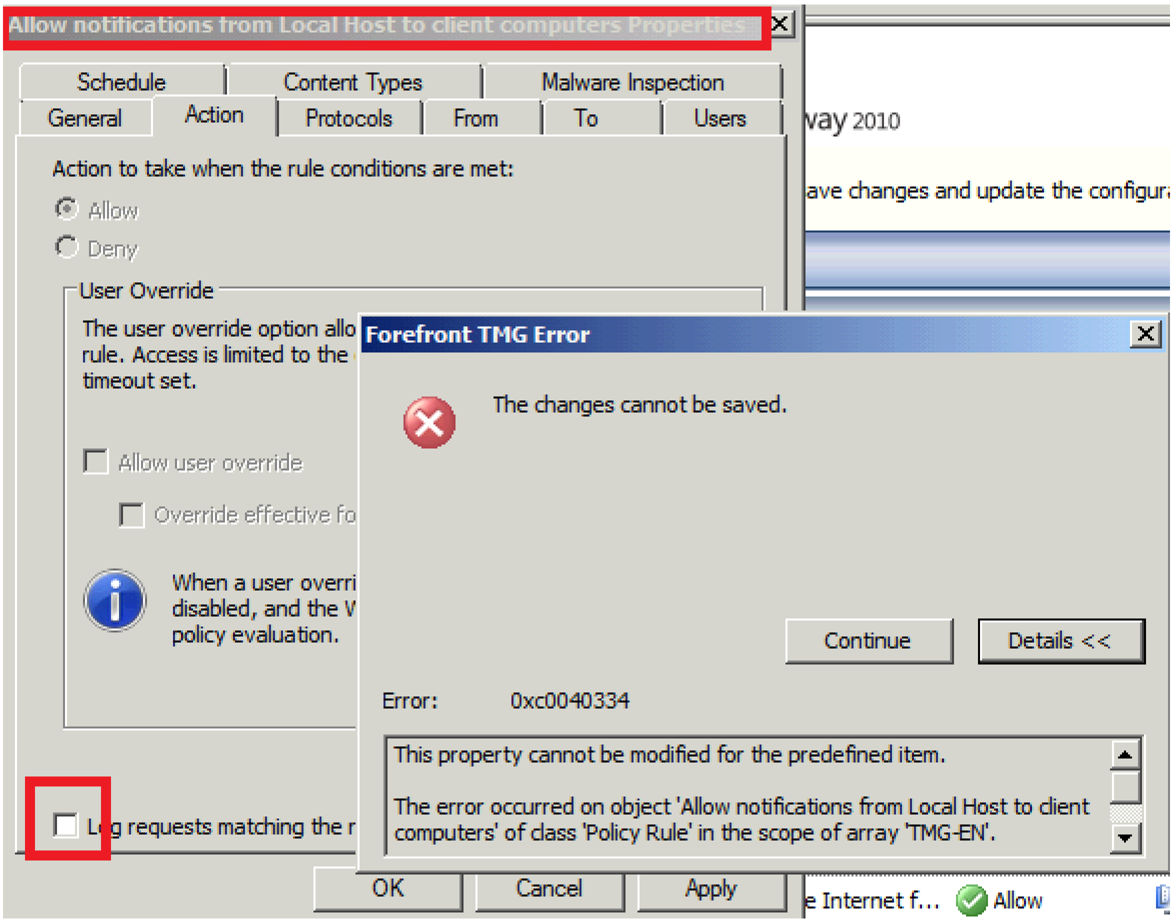
Value:

○ True
● False
○ Not set

Figure 5: Enable or disable rules with ADSIEDIT

Enable / Disable logging for System policy rules

As a next step I will show you how it is possible to disable logging for a System policy rule. If you try to disable logging for a System policy rule with the TMG MMC you will get a error message as shown in the following screenshot.



Action to take when the rule conditions are met:

● Allow

○ Deny

The user override option allo rule. Access is limited to the timeout set.

When a user overri disabled, and the W policy evaluation.

□ Log requests matching the r

ave changes and update the configur

Forefront TMG Error

The changes cannot be saved.

Error: 0xc0040334

This property cannot be modified for the predefined item.

The error occurred on object 'Allow notifications from Local Host to client computers' of class 'Policy Rule' in the scope of array 'TMG-EN'.

Figure 6: It is not possible to disable logging for this system policy rule

To overcome this limitation we must export the entire System policy rule set into a XML file.

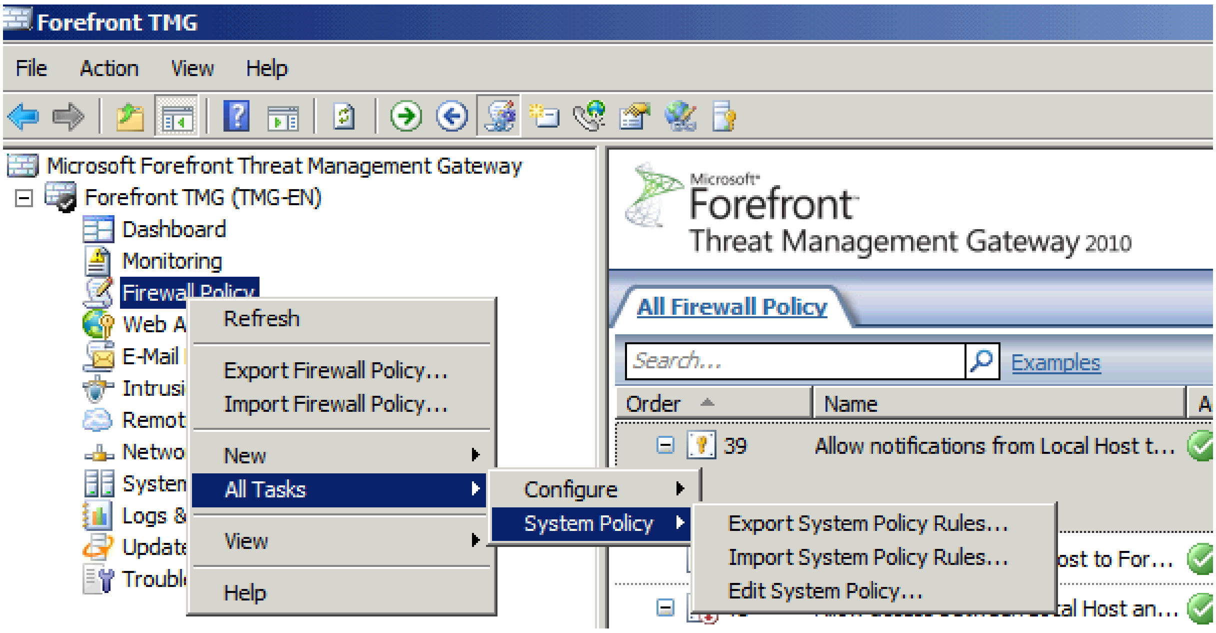
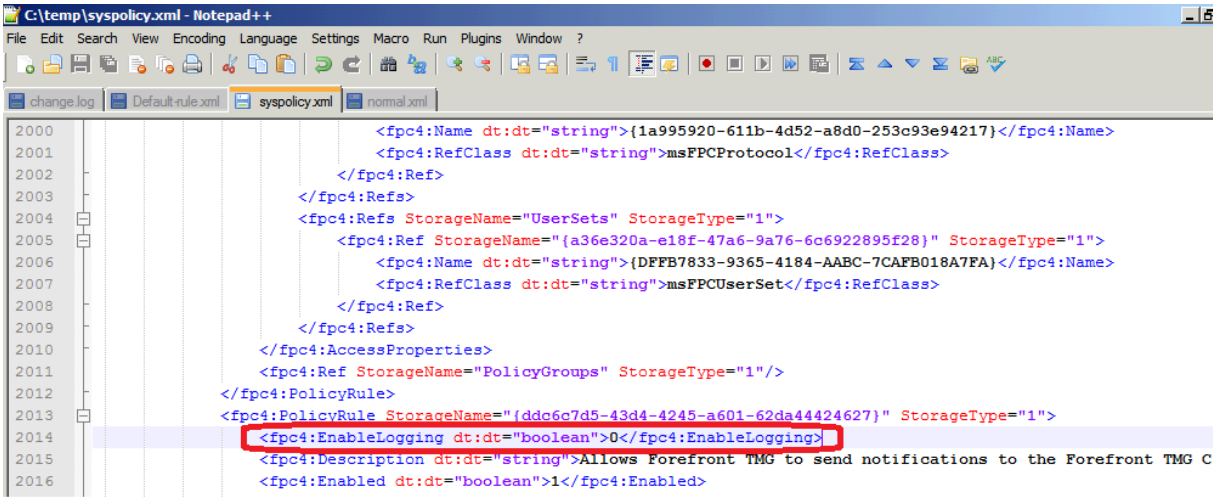


Figure 7: Export System Policy Rules

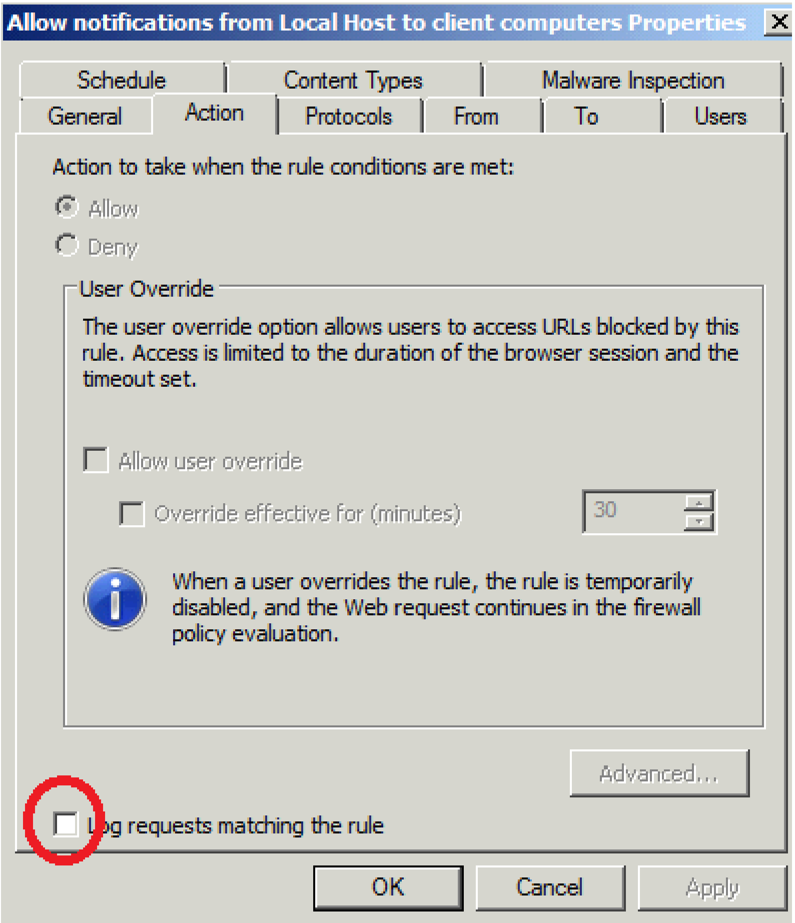
After the System policy rule set has been exported, edit the XML file with a XML editor and locate the System policy rule which you would like to change and insert the following string into the XML file as shown in the next screenshot.


C:\temp\syspolicy.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
change.log
Default-rule.xml
syspolicy.xml
normal.xml

```
                <fpc4:Name dt:dt="string">{1a995920-611b-4d52-a8d0-253c93e94217}</fpc4:Name>
                <fpc4:RefClass dt:dt="string">msFPCProtocol</fpc4:RefClass>
            </fpc4:Ref>
        </fpc4:Refs>
        <fpc4:Refs StorageName="UserSets" StorageType="1">
            <fpc4:Ref StorageName="{a36e320a-e18f-47a6-9a76-6c6922895f28}" StorageType="1">
                <fpc4:Name dt:dt="string">{DFFB7833-9365-4184-AABC-7CAFB018A7FA}</fpc4:Name>
                <fpc4:RefClass dt:dt="string">msFPCUserSet</fpc4:RefClass>
            </fpc4:Ref>
        </fpc4:Refs>
    </fpc4:AccessProperties>
    <fpc4:Ref StorageName="PolicyGroups" StorageType="1"/>
</fpc4:PolicyRule>
<fpc4:PolicyRule StorageName="{ddc6c7d5-43d4-4245-a601-62da44424627}" StorageType="1">
    <fpc4:EnableLogging dt:dt="boolean">0</fpc4:EnableLogging>
    <fpc4:Description dt:dt="string">Allows Forefront TMG to send notifications to the Forefront TMG C
    <fpc4:Enabled dt:dt="boolean">1</fpc4:Enabled>
```

Figure 8: Disable logging for this System Policy Rule

Save the XML file and import the System policy rule set with the TMG MMC. After the XML file has been imported, logging for this System policy rule has been deactivated.



Action to take when the rule conditions are met:

● Allow

○ Deny

User Override

The user override option allows users to access URLs blocked by this rule. Access is limited to the duration of the browser session and the timeout set.

□ Allow user override

□ Override effective for (minutes) 30

When a user overrides the rule, the rule is temporarily disabled, and the Web request continues in the firewall policy evaluation.

□ Log requests matching the rule

Figure 9: Logging is now disabled for this System Policy Rule.

Attention: If you try to enable logging again for this System policy rule with the Forefront TMG Management console, you will get an error that this is not possible, so you have to enable logging for this rule again with modifying the rule with an editor and after that, import the Firewall policy rule again into the TMG MMC.

Conclusion

I hope that you now have a better understanding about the Forefront TMG capabilities to export and import parts of the Forefront TMG configuration and how to modify some settings to tweak the Forefront TMG configuration. I also tried to give you some more information about the structure of Forefront TMG XML files to better understand the structure of these files. Before you start to tweak your TMG configuration, you should always make a backup of your configuration.

Related links

Microsoft Forefront TMG - Backup and Restore Capabilities
http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Backup-Restore-Capabilities.html
Backing up the Forefront TMG configuration
http://technet.microsoft.com/en-us/library/cc984454.aspx
Exporting and Importing a Forefront TMG Configuration
http://msdn.microsoft.com/en-us/library/dd435786.aspx
Importing Hammer of God Country IP Block Network Sets into ISA Enterprise Policies
http://tmgblog.richardhicks.com/2009/01/05/importing-hammer-of-god-country-ip-block-network-sets-into-isa-enterprise-policies/
Notepad++
http://notepad-plus-plus.org/
Forefront TMG – Modifying TMG System Policy rules with TMG Export / Import functionality
http://www.it-training-grote.de/download/tmg-rules-xml.pdf
Forefront TMG - Scripting with VBScript and PowerShell
http://www.isaserver.org/tutorials/Forefront-TMG-Scripting-with-VBScript-Powershell.html
Microsoft Forefront TMG – TMG Storage 101
http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Storage-101.html