

Microsoft Forefront TMG – Scripting with VBScript and PowerShell

Abstract

In this article I will give you a quick introduction how to administer Forefront TMG with VBScript and how to gather information with the “read only” PowerShell support in Forefront TMG.

Let's begin

First, I must let you know that I'm not a Scripting and programming Guru. At the beginning of the nineties I tried to learn COBOL and C, but the result was not really successful☺. Over the years I only used sample scripts to automate administrative work and beginning with the PowerShell I often use the PowerShell in Exchange environments. But I think that this article will give you enough information to understand the power of VBScript and PowerShell for Forefront TMG, so it should be easy for you to build your own scripts. We will also have a look in the Forefront TMG SDK, which comes with a small bunch of very helpful preconfigured scripts to automate some administrative work.

Forefront TMG an COM

COM is used by scripting technologies like VBScript to access Forefront TMG programmatically. Based on Wikipedia (Source: http://en.wikipedia.org/wiki/Component_Object_Model) COM is short for Component Object Model. Component Object Model (COM) is a binary-interface standard for software componentry introduced by Microsoft in 1993. It is used to enable interprocess communication and dynamic object creation in a large range of programming languages. The term COM is often used in the Microsoft software development industry as an umbrella term that encompasses the OLE, OLE Automation, ActiveX, COM+ and DCOM technologies. COM is an interface technology defined and implemented as standard only on Microsoft Windows and Apple's Core Foundation 1.3 and later plug-in API that in any case implement only a subset of the whole COM interface. For some applications, COM has been replaced at least to some extent by the Microsoft .NET framework, and support for Web Services through the Windows Communication Foundation (WCF). However, COM objects can be used with all .NET languages through .NET COM Interop.

The Forefront TMG COM has a root object called FPC.Root. The root object manages the Enterprise object which is identified as FPCEnterprise and the Arrays as FPCArrays. FPC.Root is the root of the administration COM object hierarchy, and provides programmatic access to other FPC objects.

Each Forefront TMG computer is associated with a single array as one of many fpcServer objects within the fpcServers collection.

Other objects that are managed by the Enterprise object and the Array object:

- Admin Security object (used by Enterprise and Array)

- Extensions object (used by Enterprise and Array)
- Policy Rule object (used by Enterprise and Array)
- Server object (used by Array)
- Rule Elements object (used by Enterprise and Array)
- Cache object (used by Array object)
- Network Configuration object (used by Enterprise and Array)
- Array Policy object (used by Array)
- IP object (used by Array)

Based on this knowledge you should have a better understanding about the VBScript script examples which you can find on several Internet websites and in the Forefront TMG SDK. An understanding of COM objects is also helpful when you use the PowerShell to query Forefront TMG objects. Forefront TMG has no built-in PowerShell CMDLets and will use COM.

Forefront TMG SDK

We will start with the Forefront TMG SDK, which is downloadable for free at the Microsoft website. You will find the link to download the SDK at the end of this article. The Forefront TMG SDK comes with a very helpful documentation about programming Forefront TMG but also with some advanced information about internal Forefront TMG concepts. The Forefront TMG SDK comes also with some scripting examples and I will give you some of the script examples.

The screenshot shows the 'Forefront TMG Administration Script Samples' page. It includes a table with the following data:

Name	Description
ActiveSessions.vbs	A script that creates and executes a query on the <code>FPCSessionsMonitor</code> collection for the active sessions of the <code>Microsoft Firewall Service</code> and displays the active sessions that existed when the query started.
AddAdmin.vbs	A script that adds a specific user as an administrator with permissions to monitor the Forefront TMG computer and network activity, for example, to view logs and reports, but not to configure any specific monitoring functionality.
AddCacheRule.vbs	A script that creates a new URL set in the URL sets collection of the proxy server, adds URLs to the URL set, and creates two new cache rules for caching content with a fixed <code>Time-to-Live (TTL)</code> range from all sites on the External network except the sites in the new URL set.
AddConnectivityVerifier.vbs	A script that creates a new connectivity verifier.
AddRuleAndUrlSet.vbs	A script that creates a new URL set in the URL sets collection, adds URLs to the URL set, creates a new access rule, and adds the new URL set to the objects referenced in the <code>URL Sets</code> property of the access rule.
ConfigureAlerts.vbs	A script that retrieves the collection of alerts defined in the containing <code>array</code> , iterates through the collection, and sets the e-mail address associated with each alert definition.
ConnectToCSS.vbs	A script that connects to the Configuration Storage server specified by the user using the credentials of the logged-on user, the credentials of a specified enterprise administrator with read-write permissions for accessing the stored enterprise configuration, or the credentials of a specified enterprise auditor with read-only permissions for accessing the stored enterprise configuration. The script then displays the name of the enterprise and disconnects from the Configuration Storage server (not applicable to Forefront TMG Medium Business Edition).
ControlAccessByScheduleAndUserSet.vbs	A script that creates the access rules, user set, and URL set needed to allow a specific group of workers in an organization restricted access to the Internet. The group is allowed to access only the sites listed in the URL set and only during the hours specified in the <code>Work hours</code> schedule supplied with Forefront TMG. All other workers using computers that belong to the Internal network are granted unlimited access to the Internet.
CreateEnterprisePolicy.vbs	A script that connects to the Configuration Storage server specified by the user using the credentials of the logged-on user or the credentials of a specified user that has the permissions needed to modify the stored enterprise configuration, and creates a new enterprise policy with the name specified by the user (not applicable to Forefront TMG Medium Business Edition).
HttpFilterConfig.vbs	A script that exports the configuration for the HTTP Filter Web filter from the corresponding vendor parameters set of the specified policy rule to the specified file, or imports the configuration for the HTTP Filter Web filter from the specified file to a new vendor parameters set of the specified policy rule.
ImportExport.vbs	A script that exports the configuration of the array for a Forefront TMG computer to a specified XML file or imports the configuration in a specified XML file to the array object of the Forefront TMG computer.
SetNetworkRelation.vbs	A script that creates a new network rule that defines a NAT relationship between any network belonging to the predefined All Protected Networks network set and the External network. This rule will apply to any new perimeter network created in the future because such a network will be included automatically in the All Protected Networks network set.
ShowICMPSystemPolicy.vbs	A script that retrieves the collection of system policy rules defined for an Forefront TMG computer and then implicitly uses the <code>NewEnum</code> property to iterate through the collection and display the names of the system policy rules for ICMP along with the user sets to which each rule applies.

Figure 1: Forefront TMG SDK – Script examples

One of the sample scripts allows you to add Forefront TMG Administrators to the role based access model of Forefront TMG, but only to the Monitor group. Feel free to enhance the script to add Administrator the other Forefront TMG roles.

```

Administrator: Command Prompt
C:\temp>cscript AddAdmin.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Usage:
  AddAdmin.vbs UserName

  UserName - Account name of the group or user
             (can be in domain\user-name format)

C:\temp>cscript AddAdmin.vbs trainer\marcimarc
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Done!
C:\temp>

```

Figure 2: Add a user to the Monitor role group on Forefront TMG

VBScript examples

The easiest way to automate some tasks in Forefront TMG is to use VBScript. VBScript was also available in previous version of Forefront TMG and can be used to automate some administration tasks. The first script example will show you all Forefront TMG arrays.

The script starts with configuring the Forefront TMG root which is always the FPC.Root and will set a variable which will contain the Forefront TMG arrays (objFPC.Arrays) The script will display a InputBox to enter the name of the Forefront TMG array or leaving the dialog box blank to get a list of all Forefront TMG arrays.

```

get-array.vbs - Notepad
File Edit Format View Help
set root = wscript.CreateObject("FPC.Root")
set collArrays = objFPC.Arrays
strArrayName = InputBox("Please enter the array name, or <ENTER> for the containing array:",
If strArrayName = "" Then
  'cancel option. Note that this should read "Exit Function" if used in a function.
  Exit Sub
Else
  On Error Resume Next
  Set objArray = objArrays(strArrayName)
  If Err.Number <> 0 Then
    WScript.Echo "The specified array was not found"
    Exit Sub
  End If
  On Error GoTo 0
End If

```

Figure 3: Display Forefront TMG array information

Scripting classic

A real classic script which I often use in ISA Server and Forefront TMG implementations is to export the entire Forefront TMG configuration via script. You can use this script with the Windows Task Scheduler to export the entire Forefront TMG configuration to another host at repeating intervals.

```

Dim fileName
Dim WSHNetwork
Dim shareName: shareName = WScript.Arguments(0)

```

```

Dim xmldom : set xmldom = CreateObject("Msxml2.DOMDocument")
Dim fpc : set fpc = WScript.CreateObject("Fpc.Root")
Dim array : set array = fpc.GetContainingArray
set WSHNetwork = CreateObject("WScript.Network")
fileName=shareName & "\" & WSHNetwork.ComputerName & "-" &
Month(Now) & "-" & Day(Now) & "-" & Year(Now) & ".xml"
array.Export xmldom, 0
xmldom.save(fileName)

```

The script uses the Windows Scripting Host (WSH), defines the Forefront TMG Root (FPC.Root), sets some variables and creates an XML file based on the current day when the script has been executed. Save the scripting example as a file with the .VBS extension and create a batch file with the following syntax:

```
Cscript TMGBACKUP.VBS \\RemoteServer\TMG-BACKUP
```

This will create a backup of your Forefront TMG configuration in the specified file share (TMG-Backup). If you want to create recurring backups of your Forefront TMG configuration create a task with the Windows Task Scheduler, which executes the batch file.

Exporting the ISA Server 2006 VPN configuration and import into Forefront TMG

The following example is a little bit of more complexity and exports the ISA Server 2006 VPN configuration to import this configuration on a Forefront TMG Server. My MVP colleague Christian Groebner has created this script. The complete article can be found on <http://www.msisafaq.de> a German noncommercial website dedicated to ISA Server and Forefront TMG.

If you want to use this script example copy the entire text into Notepad and save it with the .VBS extension.

```

#####
#####

Dieses Skript übernimmt die IPSec-Einstellungen für Phase I und II der IPSec-VPN-Tunnel
aus der ISA Server 2006-Konfiguration nach dem Import und wendet diese auf die
Konfiguration
von Microsoft TMG an.

Die Verwendung dieses Skripts erfolgt auf eigene Verantwortung.
Es wird keine Haftung für eventuelle Schäden übernommen!

Geschrieben von Christian Gröbner [MVP Forefront]
#####
#####

' ----- Sub restore_ipsec_settings -----

Sub restore_ipsec_settings(fpcRoot, VPN_Name, Int_PhaseI, Enc_PhaseI, Int_PhaseII,

```

```
Enc_PhaseII)
```

```
Dim Intproviders  
Dim Encproviders
```

```
Intproviders = Array("SHA1","MD5")  
Encproviders = Array("DES","3DES")
```

```
set objIPSec =  
fpcRoot.GetContainingArray.NetworkConfiguration.Networks.Item(VPN_Name).VPNConfiguration.IPSecSettings
```

```
wscript.echo "Restoring IPSec-settings for network" & VPN_Name & vbCrLf  
wscript.echo "Phase I integrity : " & Intproviders(Int_PhaseI)  
objIPSec.Phase1Integrity = Int_PhaseI  
wscript.echo "Phase I encryption : " & Encproviders(Enc_PhaseI)  
objIPSec.Phase1Encryption = Enc_PhaseI  
wscript.echo "Phase II integrity : " & Intproviders(Int_PhaseII)  
objIPSec.Phase2Integrity = Int_PhaseII  
wscript.echo "Phase II encryption : " & Encproviders(Enc_PhaseII) & vbCrLf  
objIPSec.Phase2Encryption = Enc_PhaseII  
wscript.echo "Successfully applied the settings"  
wscript.echo "-----" & vbCrLf
```

```
End Sub
```

```
' ----- Sub Main -----
```

```
Sub Main()
```

```
Dim PhaseI_Int  
Dim PhaseI_Enc  
Dim PhaseII_Int  
Dim PhaseII_Enc  
Dim config
```

```
config = Inputbox("Please enter the complete path and filename with extension to the  
existing configuration file of ISA 2006 : (Example: C:\Temp\config.xml)")
```

```
Set xmlFile = CreateObject("Microsoft.XMLDOM")
```

```
If xmlFile.load(config) then
```

```
set objFPC = CreateObject("FPC.Root")
```

```
Set networkNodes = xmlFile.getElementsByTagName("fpc4:Network")
```

```
For each networkNode in networkNodes
```

```
If (Not(networkNode.selectSingleNode("fpc4:NetworkConnectionType") is Nothing)) Then
```

```

If (networkNode.selectSingleNode("fpc4:NetworkConnectionType").Text = 4) Then

    PhaseI_Int = 0
    PhaseI_Enc = 1
    PhaseII_Int = 0
    PhaseII_Enc = 1
    Name = networkNode.selectSingleNode("fpc4:Name").Text

    Set ipsecSettingsNode =
networkNode.selectSingleNode("fpc4:VpnNetworkConfiguration/fpc4:VpnNetworkIPSecSett
ings")

    If (Not(ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase1Encryption") is
Nothing)) Then PhaseI_Enc =
ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase1Encryption").Text
    If (Not(ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase1Integrity") is
Nothing)) Then PhaseI_Int =
ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase1Integrity").Text
    If (Not(ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase2Encryption") is
Nothing)) Then PhaseII_Enc =
ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase2Encryption").Text
    If (Not(ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase2Integrity") is
Nothing)) Then PhaseII_Int =
ipsecSettingsNode.selectSingleNode("fpc4:VpnNetworkPhase2Integrity").Text

    restore_ipsec_settings objFPC, Name, PhaseI_Int, PhaseI_Enc, PhaseII_Int, PhaseII_Enc

End If

End If

Next

objFPC.GetContainingArray.Save

Else

wscript.echo("The file does not exist!")

End If

End Sub

'----- Start the script -----

Main

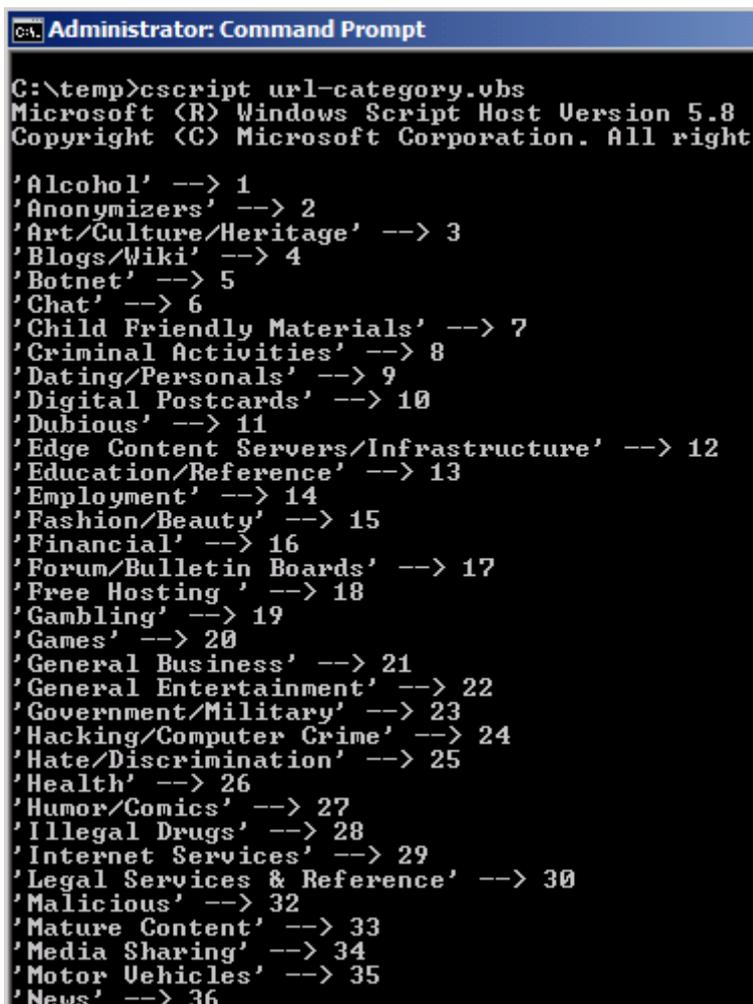
```

Display Forefront TMG URL categories

One of the new functionality in Forefront TMG is the support for dynamic URL filtering. The URL filtering uses categories. To display all the Forefront TMG URL filter categories, you must create a script with the following code:

```
set root=CreateObject("FPC.Root")
For Each cat in root.GetContainingArray().RuleElements.UrlCategories
    wscript.echo "" & cat.Name & "" --> " & cat.CategoryID
Next
```

The output of the script will be like the following screenshot.



```
C:\temp>cscript url-category.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

'Alcohol' --> 1
'Anonymizers' --> 2
'Art/Culture/Heritage' --> 3
'Blogs/Wiki' --> 4
'Botnet' --> 5
'Chat' --> 6
'Child Friendly Materials' --> 7
'Criminal Activities' --> 8
'Dating/Personals' --> 9
'Digital Postcards' --> 10
'Dubious' --> 11
'Edge Content Servers/Infrastructure' --> 12
'Education/Reference' --> 13
'Employment' --> 14
'Fashion/Beauty' --> 15
'Financial' --> 16
'Forum/Bulletin Boards' --> 17
'Free Hosting' --> 18
'Gambling' --> 19
'Games' --> 20
'General Business' --> 21
'General Entertainment' --> 22
'Government/Military' --> 23
'Hacking/Computer Crime' --> 24
'Hate/Discrimination' --> 25
'Health' --> 26
'Humor/Comics' --> 27
'Illegal Drugs' --> 28
'Internet Services' --> 29
'Legal Services & Reference' --> 30
'Malicious' --> 32
'Mature Content' --> 33
'Media Sharing' --> 34
'Motor Vehicles' --> 35
'News' --> 36
```

Figure 4: Display Forefront TMG array information

Forefront TMG and PowerShell

Forefront TMG doesn't have a built-in Windows PowerShell cmdlet, but you can use COM objects. When you have access to the ProgID of a COM component, which is stored in the Registry you can use the New-Object command in Windows PowerShell as you can see in the following screenshot (Root Object is always FPC.Root).

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.TRAINER> $TMGRoot = New-Object -comObject FPC.root
PS C:\Users\administrator.TRAINER> _

```

Figure 5: Define TMG Root Object

Display the Forefront TMG Root

After defining the Forefront TMG Root Object in the Windows PowerShell we can get information about the Forefront TMG Root Object configuration, as shown in the following screenshot.

```

Administrator: Windows PowerShell
PS C:\Users\administrator.TRAINER> $TMGRoot

Arrays                : System.__ComObject
Enterprise             : System.__ComObject
ConfigurationStorageServer : TMG-EN.trainer.intern
RequireApplyChanges   : False
ChangesMade           : False
StorageChangeNumber   : 57360
IsaEdition            : 32
VendorMode            : False
ConfigurationMode     : 0

```

Figure 6: Display Forefront TMG root

Query single Forefront TMG objects

If you want to query single Forefront TMG objects enter \$TMGRoot. in the Windows PowerShell window and hit the TAB key behind the \$TMGRoot. definition to display all elements.

```

Administrator: Windows PowerShell
PS C:\Users\administrator.TRAINER> $TMGRoot.ConfigurationStorageServer
TMG-EN.trainer.intern
PS C:\Users\administrator.TRAINER> _

```

Figure 7: Query Forefront TMG objects under the FPC.Root

Display properties of FPC.Root

```

Administrator: Windows PowerShell
PS C:\Users\administrator.TRAINER> $tmgroot | Get-Member -membertype *property

TypeName: System.__ComObject#<8bf0aefa-b4fd-4d81-8046-a069d948d673>

Name                MemberType Definition
-----
Arrays              Property   IFPCArrays Arrays () <get>
ChangesMade         Property   bool ChangesMade () <get>
ConfigurationMode   Property   FpcConfigurationMode ConfigurationMode () <get>
ConfigurationStorageServer Property   string ConfigurationStorageServer () <get>
Enterprise          Property   IFPCEEEnterprise Enterprise () <get>
IsaEdition          Property   FpcIsaEditionType IsaEdition () <get>
RequireApplyChanges Property   bool RequireApplyChanges () <get> <set>
StorageChangeNumber Property   int64 StorageChangeNumber () <get>
VendorMode          Property   bool VendorMode () <get> <set>

PS C:\Users\administrator.TRAINER>

```

Figure 8: Display properties of FPC.Root

Determine the Forefront TMG Enterprise and Array configuration with Export

Our last example how to use the PowerShell with Forefront TMG is the script example from the following source: <http://social.technet.microsoft.com/Forums/en-US/Forefrontedgegeneral/thread/f42ae1ba-2db5-4319-9b65-22a25201088a/>. This script determines the Forefront TMG Enterprise and associated arrays and exports this configuration to an XML file.

Conclusion

In this article I gave you a quick introduction how to administer Forefront TMG with VBScript and the Microsoft PowerShell. There are a lot of downloadable Script examples in the Internet and with a little bit of experience in programming techniques it should be possible to create your own scripts to ease the daily administration of Forefront TMG. I hope that the next version of Forefront TMG will come with full, not read only PowerShell support.

Related links

ISA/TMG Scripting examples

<http://www.isascripts.org>

Website with helpful ISA/TMG scripts and tools

<http://www.isatools.org>

Forefront TMG SDK

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8809cfda-2ee1-4e67-b993-6f9a20e08607&displaylang=en>

New Forefront TMG COM objects

<http://msdn.microsoft.com/en-us/library/dd447763.aspx>