Configure Forefront TMG to integrate with an TMG Array

Abstract

In this article, I will show you how to integrate Microsoft Forefront TMG into an TMG array for centrally administration purposes.

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 month ago, Microsoft released Beta 2 from Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

Before we start installing Microsoft Forefront TMG into an array, I would like to explain to you the new terminology used in Forefront TMG. There are two different terms:

- EMS (Enterprise Management Server)
- CSS (Configuration Storage Server)

EMS

The Enterprise Management Server is a server which is used to manage an TMG Enterprise Array or possible a standalone server.

CSS

The Configuration Storage Server (CSS) is used for all local TMG installations and provides the storage for the TMG Server configuration. Every TMG has a local CSS. After the TMG administrator joins the Server to an TMG Array, the local TMG Server will use the Enterprise CSS (EMS). After the local TMG server has joined the Enterprise CSS, the local CSS will be disabled.

First we have to create a new Microsoft Forefront Threat Management Gateway Enterprise. To do so, start the setup from the TMG setup installation file and select the appropriate option.



Figure 1: Create a new Microsoft Forefront Threat Management Gateway Enterprise

It is also possible to create a replica from the Enterprise configuration. This will create a new EMS server which works hand in hand with the other EMS server. An productive TMG Enterprise should always have two or more EMS Server.

You must specify an account which is used for the EMS service. In this lab, I used the Administrator account from the domain. In an production environment you should use another not so security critical account.

🙀 Microsoft Forefront Thr	eat Management Gateway Beta EE- Installation Wizard	×
Enterprise Management Server Service Account Select the account under which the Enterprise Management Server service will run.		
When installing a Enterprise Management Server on a domain controller, you must specify an account under which the Enterprise Management Server service will run. The specified account will be granted permissions to log on as a service.		
User name:	administrator	
Password:	•••••	
If the specified account does not belong to the Domain Admins group, you must perform additional steps after you complete this installation. Otherwise, Windows authentication with array members will not function properly.		
Refer to the "Enterprise Management Server on Active Directory domain controller" in the Installation Guide for detailed information.		
	< Back Next > Cancel	

Figure 2: Enterprise Management Server Service Account

The following figure give you a overview about the new Microsoft Forefront Threat Management Console with the EMS Server installed. The configuration is similar to the ISA Server 2006 Management Console, as you can see in the following screenshot.



Figure 3: New Microsoft Forefront Threat Management Gateway Enterprise and console

Next, we have to create a new TMG Array, and after that it will be possible to join standlone TMG Servers to the new TMG Array. Start creating a TMG Array by executing the wizard to create new Arrays.

New Array Wizard		×
	Welcome to the New Array Wizard	
	This wizard helps you create a new array and set array policy settings.	
	Array name: TMG-Array	
	To continue, click Next.	
	< Back Next > Cancel	

Figure 4: Wizard to create a new TMG Array

It is possible to create multiple Arrays in the TMG Enterprise, and there is a minimum of one Server per TMG Array. You must assign a name for the new Array.

New Array Wizard				×
Array DNS Name Type the Domain Name	System (DNS) nam	ne of the array.		A
Type the DNS name used b TMG array.	y Firewall clients a	nd Web clients	when connecting t	o this Forefront
Аттау's DNS name:	TMG-Array.doma	in.local		
		< Back	Next >	Cancel

Figure 5: Specify the Array DNS Name

As a next step, every Array must have a resolvable DNS name. The DNS name is used by the TMG Server Firewall Client and the Webproxy client. You must create a corresponding DNS record in your internal DNS Server for the TMG Array servers.

Every Array must have an Enterprise Policy. Select the default Policy or better a newly created Enterprise Policy which should be used in the Array.

New Array Wizard	X
Assign Enterprise Policy Specify which enterprise policy to apply to this array.	\mathbb{A}
Select the enterprise policy to apply to this new array:	
Default Policy	
Note that the "Default Policy" includes the built in "Deny All" enterprise rule only. Rules for this policy should be defined in the Array Firewall Policy.	
< Back Next >	Cancel

Figure 6: Assign an Enterprise Policy

Now it is time to select which type of Array Firewall policy rules can be created for the Array.

New Array Wizard	×
Array Policy Rule Types Use this page to specify the types of array firewall policy rules that can be created for this array.	
Select the types of array firewall policy rules that can be created for this array:	
 "Deny" access rules "Allow" access rules Publishing rules (Deny and Allow) 	
< Back Next > 0	Cancel

Figure 7: Specify Array Policy Rule Types

It takes some time to create the new TMG Array, depending on the performance of your system.

New Array Wizard		×
	Completing the New Array Wizard	
	You have successfully completed the New Array Wizard. The new array will have the following configuration:	
Create New Array		
Creating the new array	<u>OK</u>	
	To close this wizard, click Finish.	
	< Back Finish Cancel	

Figure 8: Create a new Array process

After some minutes, the TMG Array should be created sucessfully as you can see in the following screenshot. It is now possible to join the standlone TMG servers to the TMG Enterprise.



The installation of Microsoft Forefront TMG is part of other articles on www.isaserver.org so I only created one screenshot about the installation process to see which setup option you must choose in the TMG installation wizard.

🙀 Microsoft Forefront Threat Manageme	ent Gateway	Beta EE- Installa	tion Wizard	×
Setup Scenarios				
Select the Forefront Threat Management G computer.	ateway installa	tion option for this		
Install Forefront Threat Management	ent Gateway	services		
The computer will run Forefront Threat Management Gateway services. Forefront Threat Management Gateway Management will be installed for local management of this Forefront Threat Management Gateway computer.				
C Install Forefront Threat Manageme	ent Gateway	Management on	ly	
The computer will be used to remotely manage computers running Forefront Threat Management Gateway.				
O Install Enterprise Management Server				
The computer will provide centralized management for Forefront Threat Management Gateway arrays. Enterprise-level firewall policies and policy objects can be defined.				
	< Back	Next >	Cancel	

Figure 10: Installing TMG

After the TMG setup has successfully finished, start the Microsoft Forefront Threat Management console and click the Join Array option in the task pane as shown in the following screenshot.



Figure 11: Start the Join Array Wizard

The Join Array Wizard starts



Figure 12: Join Array Wizard

Select the Array Membership type. Because we prviously created an Enterprise Management Server and a TMG Array, we will join the standlone TMG server to the EMS.



Figure 13: Join an array managed by an EMS Server

Specify the fully qualified domain name (FQDN) for the the EMS. It is also possible to change the account which has the rights to connect to the EMS server.

Join Array Wizard		×
Enterprise Management Select the EMS server and selected server.	Server Details nd specify the user account used to connect to	o the
EMS fully qualified domain na	me (FQDN):	
vv2k8-EX2k7.domain.iocai		browse
User account with rights to	connect to the EMS server	
Connect using the cr	edentials of the logged on user	
C Connect using this ac	count:	
User name:		1
Password:		
	< Back Next >	Cancel

Figure 14: Specify the EMS FQDN

Because we already created an TMG Array in the EMS, we will select the previously created TMG Array. It is also possible to create a new Array, but this could take a longer time as creating the Array on the EMS Server because of network latency.

Join Array Wizard X		
Join EMS Managed Array This server can join an existing EMS managed array, or you can create and join a new EMS managed array.		
Select the EMS managed array options:		
O Join an existing EMS managed array (recommended):		
Select array: TMG-Array		
To join an array you must have Forefront TMG Array Administrator privileges for the specified array.		
Create a new EMS managed array. Note that creating a new array may take significant time due to network latency.		
< Back Next > Cancel		

Figure 15: Join an existing EMS array

The TMG standalone server is now joining the TMG Array.

Join Array Wizard		×
ti 'c	Completing the Join Array Wizard	le ks
	You have successfully completed the Join Array Wizard. The following settings will be applied:	
Join array		
Joining the array		ОК
KKK		rk
ØKAN -		ľ
	< Back Finish	Cancel d

Figure 16: Join the array phase

After some time, the TMG standalone Server is now a member of the EMS Array.

Join array	
You have successfully joined the array	ОК

Figure 17: Array successfully joined

Start the TMG Management console and navigate to the properties of the newly Array joined TMG server and you will see that the TMG server is now managed by the EMS array.

W2K8-TMG1 Properties	? ×
General CARP Communication	Product ID
W2K8-TMG1	
Full computer name:	
W2K8-TMG1.domain.local	
(optional):	
Configuration Management:	EMS Managed array
Forefront TMG version:	
Product ID:	00143-OEM-7010373-76340
Created:	21.05.2009 15:14:12
Installation directory:	C:\Program Files\Microsoft ISA Ser
Host ID	3
C	K Cancel Apply

Figure 18: EMS Array information

To see which CSS (Configuration Storage Server) is used by the TMG Server, navigate to the TMG Array properties, click the Configuration Storage tab. If you have a second CSS Server, which is recommended, enter the additional CSS Server as an alternate Configuration Storage Server.

TMG-Array Properties	<u>' ×</u>
Assign Roles Customer Feedback Join Microsoft Telemetry Servic Published Configuration Storage Intra-Array Credentials General Policy Settings Configuration Storage Specify the Configuration Storage server used to store the array configuration. When the specified server is unavailable, the alternate server	r
will be used. Configuration Storage server (enter the FQDN): W2k8-EX2k7.domain.local Browse Alternate Configuration Storage server (optional):	
Browse Check the Configuration Storage server for updates every: 15 seconds	
Select the authentication type used for connections between Forefront TM and the Configuration Storage server: Windows authentication Select	G
To save these settings, this computer must be able to connect to the specified Configuration Storage servers.	
OK Cancel Apply	

Figure 19: TMG Array properties

After joining the Server to the TMG Array, you can now configure TMG for your business needs.

Conclusion

In this article, I gave you an overview about how to integrate the Microsoft Forefront Threat Management Gateway into an TMG array to centrally manage all TMG servers within the TMG Enterprise or Array. There are not a lot changes from ISA Server 2006 Enterprise CSS concepts, so you should be quickly familiar with the EMS console in Microsoft Forefront TMG.

Related links

Forefront Threat Management Gateway Beta 2 http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0fa5db-8f236995bccd&DisplayLang=en Forefront TMG Beta 2 is Released http://blogs.technet.com/isablog/archive/2009/02/06/forefront-tmg-beta-2-isreleased.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