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

Microsoft Forefront TMG – Role based Administration

Abstract

In this article I will show you how to implement a role based administration model with Microsoft Forefront TMG Standard and Enterprise for delegated administration.

Let's begin

Forefront TMG allows the delegation of administrative permissions to individual users to make the administration model more flexible. Forefront TMG uses two different models to assign permissions to individual users. Permissions can be assigned at the Enterprise level (if Forefront TMG has been joined to an Enterprise array) and at the Array level. A standalone Forefront TMG server can also be used to assign different administrative permissions.

Forefront TMG implements access control to all parts of the TMG configuration in form of Windows Server 2008 security descriptors. The discretionary access control list (DACL) in the security descriptor (SD) of each object defines the types of access, or permissions that can be granted to users and groups.

For delegated administration of Forefront TMG it is possible to assign users and groups to administrative roles in Forefront TMG. An administrative role defines a collection of rights, which a user or group requires to perform Forefront TMG administration. When a role is assigned to a user or group, Forefront TMG configures the DACLs in the security descriptors of the corresponding objects to grant the permissions needed to perform the actions allowed by the role to the user or group. Forefront TMG also reconfigures the DACLs when you modify the administrative roles or when you restart the Microsoft Forefront TMG Control service (isactrl).

Using role-based administration

You can use administrative roles to organize Forefront TMG administrators into separate, predefined roles which have different rights to perform Forefront TMG management tasks.

Roles can be assigned to any Windows user or group but you should give only trusted Administrators the necessary permission to do their work. Every change in the administrative role model will be stored in the Active Directory Lightweight directory instance, called AD-LDS in Windows Server 2008 and above. The changes in the AD-LDS configuration will be applied to every EMS (Enterprise Management Server) in the TMG Enterprise.

Please note:

Administrative roles should not be assigned to the CREATOR OWNER or CREATOR GROUP, because AD-LDS doesn't know these security principals.

Attention:

As with ISA Server 2006, if you want to allow a Forefront TMG Administrator to view the Forefront TMG performance monitor counters, the account used must be member of the Windows Server 2008 Performance monitor user group.

Administrative roles at the Array level

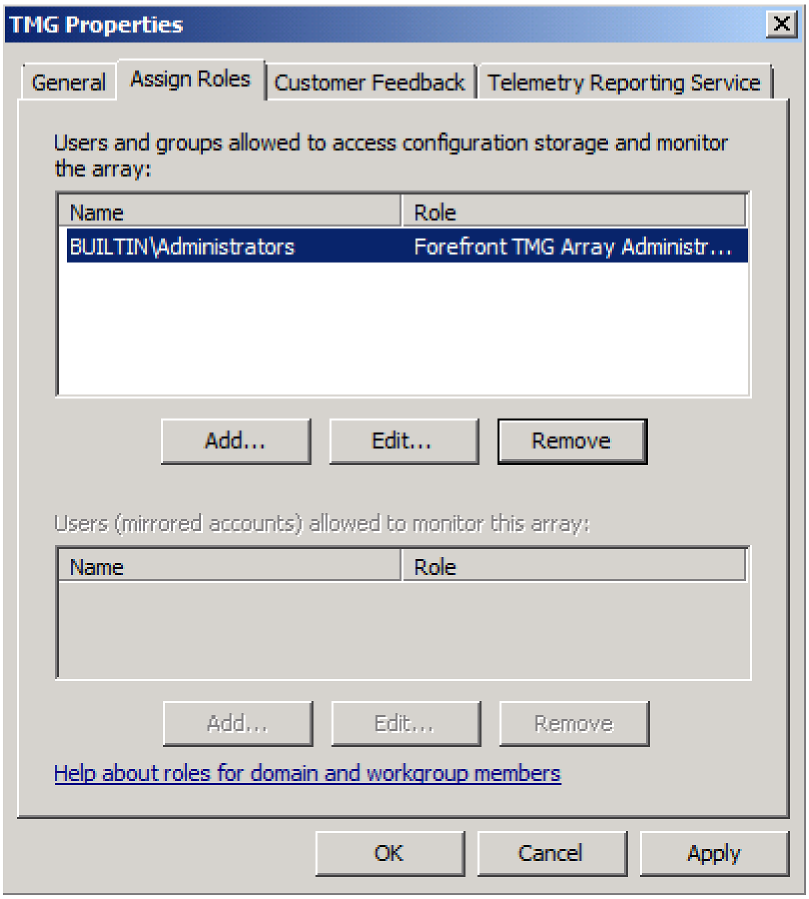
Forefront TMG supports multiple Forefront TMG arrays within one TMG Enterprise and it is possible to define different administrative roles at each array separately.

The following table describes the administrative roles at TMG array level:

Role	Description
Forefront TMG Array Monitoring Auditor	Members of this role are allowed to monitor the Forefront TMG Servers in the array and the network connectivity but are not allowed to view the Forefront TMG configuration
Forefront TMG Array Auditor	Members of this administrative role have more permission. Role members are allowed to perform all monitoring tasks (Alert and log configuration). Members of this group are also allowed to view (but not to modify) the Forefront TMG configuration
Forefront TMG Array Administrator	Members of this role have full administrative control above all Forefront TMG servers in the TMG array

Table 1: TMG administrative roles at Array level

If you want to assign additional permissions to manage Forefront TMG, start the TMG management console, navigate to the array properties and select the “Assign roles” tab as shown in the following picture.



Users and groups allowed to access configuration storage and monitor the array:

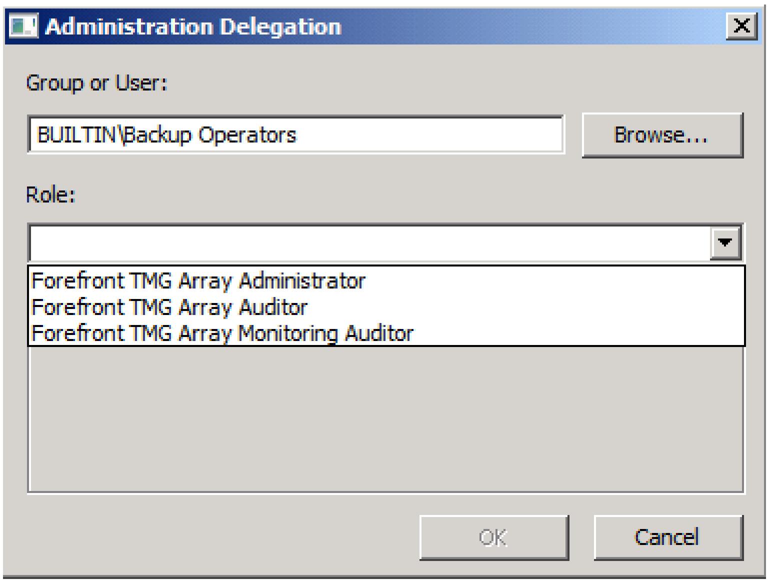
Name	Role
BUILTIN\Administrators	Forefront TMG Array Administr...

Users (mirrored accounts) allowed to monitor this array:

Name	Role

Figure 1: Assign Forefront TMG roles to a user group

The following screenshot shows how to assign Forefront TMG administrative roles:


Administration Delegation
Browse...
Forefront TMG Array Administrator
Forefront TMG Array Auditor
Forefront TMG Array Monitoring Auditor
OK
Cancel

Group or User: BUILTIN\Backup Operators

Role:

Figure 2: Assign Forefront TMG roles to a user group

Specific role permissions

The following table lists all permission for every Forefront TMG array role:

Action	Forefront TMG Array	Forefront TMG Array Auditor	Forefront TMG Array

	Monitoring Auditor		**Administrator**
View Dashboard, alerts, connectivity, sessions, services	Allowed	Allowed	Allowed
Acknowledge and reset alerts	Allowed	Allowed	Allowed
View log information	Not Allowed	Allowed	Allowed
Create alert definitions	Not allowed	Not allowed	Allowed
Create reports	Not allowed	Allowed	Allowed
Stop and start sessions and services	Not allowed	Allowed	Allowed
View firewall policy	Not Allowed	Allowed	Allowed
Configure firewall policy	Not allowed	Not allowed	Allowed
Configure cache	Not allowed	Not allowed	Allowed
Configure a virtual private network (VPN)	Not allowed	Not allowed	Allowed
Drain and stop network load balanced (NLB) firewall or Web Proxy load balanced server	Not allowed	Allowed	Allowed
View local configuration (in ADAM on array member)	Not allowed	Allowed	Allowed
Change local configuration (in ADAM on array member)	Not allowed	Not allowed	Not allowed

Least privileges

You should always grant permissions by the least privilege principle, because Forefront TMG is your central protection against attacks from the Internet and external (not tusted) networks.

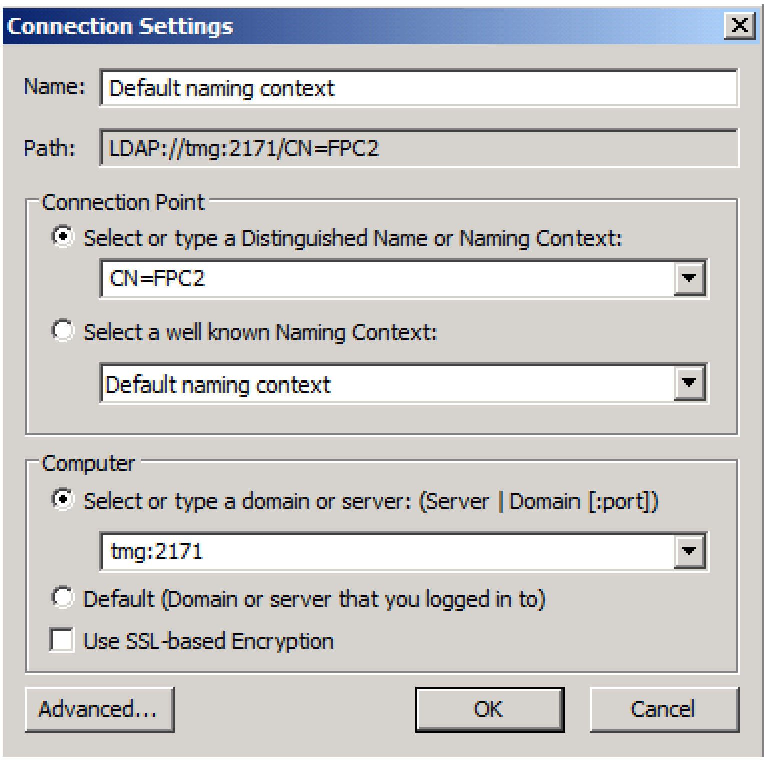
Limit Guest accounts

It is not recommended to use the built in guest account, because the guest account will be granted access to the “all authenticated users” group, so if you enable the guest account (deactivated by default), the guest account has all permissions granted to the “all authenticated users” group.

Forefront TMG administrative roles in AD-LDS

As explained above in this article, Forefront TMG saves the TMG configuration and the administrative roles in the local AD-LDS instance or in the central EMS (Enterprise Management Server) AD-LDS database.

If you want to see the administrative roles in AD-LDS, we must connect to the AD-LDS instance. To do so, start ADSIEDIT.MSC and connect to the AD-LDS instance on port 2171. The AD-LDS configuration of Forefront TMG can be opened by the common name (CN) called FPC2. The next screenshot tells you how to open an AD-LDS connection to the Forefront TMG configuration:



Connection Settings

Name: Default naming context

Path: LDAP://tmg:2171/CN=FPC2

Connection Point

● Select or type a Distinguished Name or Naming Context:

CN=FPC2

○ Select a well known Naming Context:

Default naming context

Computer

● Select or type a domain or server: (Server | Domain [:port])

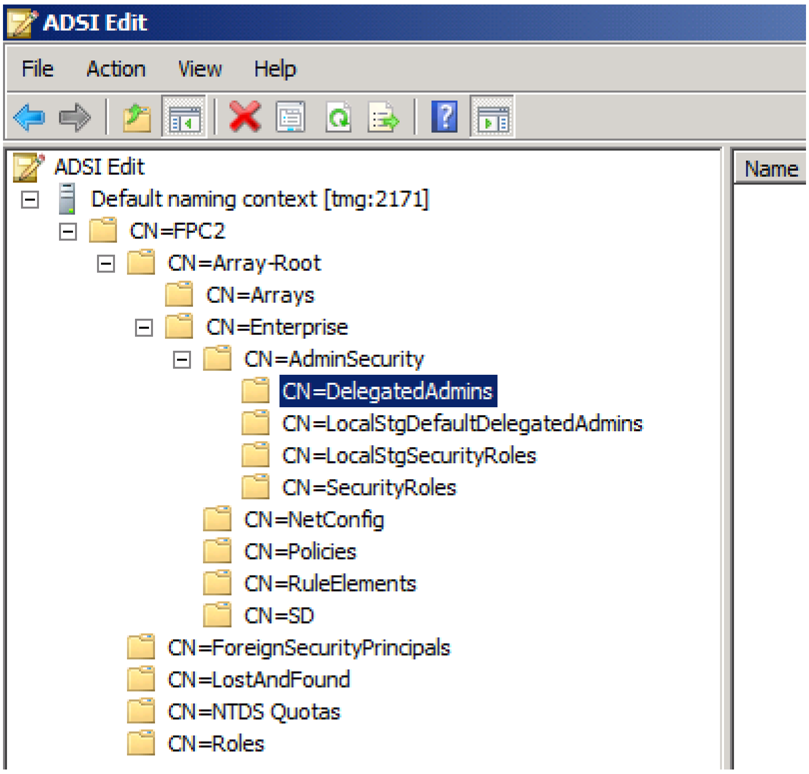
tmg:2171

○ Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

Figure 3: Connect to the AD-LDS instance of Forefront TMG

Navigate to CN=Arrays or CN=Enterprise to see the configuration of Forefront TMG stored in AD-LDS. Under the Common Name “Admin Security” you will see the predefined delegated administrative roles in the CN=DelegatedAdmins section



ADSI Edit
- Default naming context [tmg:2171]
  - CN=FPC2
    - CN=Array-Root
      - CN=Arrays
      - CN=Enterprise
        - CN=AdminSecurity
          - CN=DelegatedAdmins
          - CN=LocalStgDefaultDelegatedAdmins
          - CN=LocalStgSecurityRoles
          - CN=SecurityRoles
        - CN=NetConfig
        - CN=Policies
        - CN=RuleElements
        - CN=SD
    - CN=ForeignSecurityPrincipals
    - CN=LostAndFound
    - CN=NTDS Quotas
    - CN=Roles

Figure 4: DelegatedAdmins in AD-LDS

Administrative roles at the Forefront TMG Enterprise

If the Forefront TMG Server has joined a Forefront TMG Enterprise array managed by an Enterprise Management Server, it is also possible to delegate permissions to administer the entire Forefront TMG Enterprise.
Forefront TMG comes with two built-in administrative roles at the Enterprise level:

Forefront TMG Enterprise Administrator

Members of this administrative role in Forefront TMG are allowed to perform all administrative tasks in the Enterprise and within TMG arrays in the Enterprise.

Forefront TMG Enterprise Auditor

Users and groups which are members of this administrative role are allowed to perform Forefront TMG monitoring tasks for the TMG Enterprise and every Forefront TMG array.

The way to assign users and groups to these administrative roles in Forefront TMG at the Enterprise level is the same as assigning permissions at the TMG array level.

Conclusion

In this article, I tried to give you an overview about how to implement an administration model to delegate permissions to administer Microsoft Forefront TMG Standard and Enterprise. The administration model in Forefront TMG allows you to use a few predefined roles to administer different parts of Microsoft Forefront TMG. I like the view only administrator role to give special people only read only access to the Forefront TMG configuration. This role is great for people with auditing requirements which doesn’t require more permission than necessary.

Related links

Planning permissions and roles
http://technet.microsoft.com/en-us/library/cc995242.aspx
Configuring roles and permissions
http://technet.microsoft.com/en-us/library/dd441007.aspx