Use the Security Configuration Wizard with TMG 2010

In this article, I will show you how to use the Security Configuration Wizard with Microsoft Forefront Threat Management Gateway 2010.

In this article, I will show you how to use the Security Configuration Wizard with Microsoft Forefront Threat Management Gateway 2010.

Windows Server 2008 and 2008R2 have a tool called the Security Configuration Wizard (SCW). This is a tool that can be used to simplify the basic operating system 'consolidation' task to prepare for the Forefront Threat Management Gateway (TMG) 2010 firewall deployment. SCW will create a policy to use Configure services, verify policies and some registry settings based on the roles and features installed. In this article, I will show you how to use the SCW to configure a security policy on the TMG firewall system, how to implement this security policy with Active Directory Group Policy.

The Forefront TMG role for SCW

By default, SCW does not support the TMG 2010 role or TMG Enterprise Management Server (EMS) role. To support these roles, you need to download and install the **TMGRolesForSCW.exe** file found in TMG 2010 Tools and Software Development Kit (SDK), here.

Install the TMG Role for SCW

To install the TMG Role for SCW, you need to run the executable file **TMGRolesForSCW.exe** .

Figure 1

Accept the items in the registration agreement.

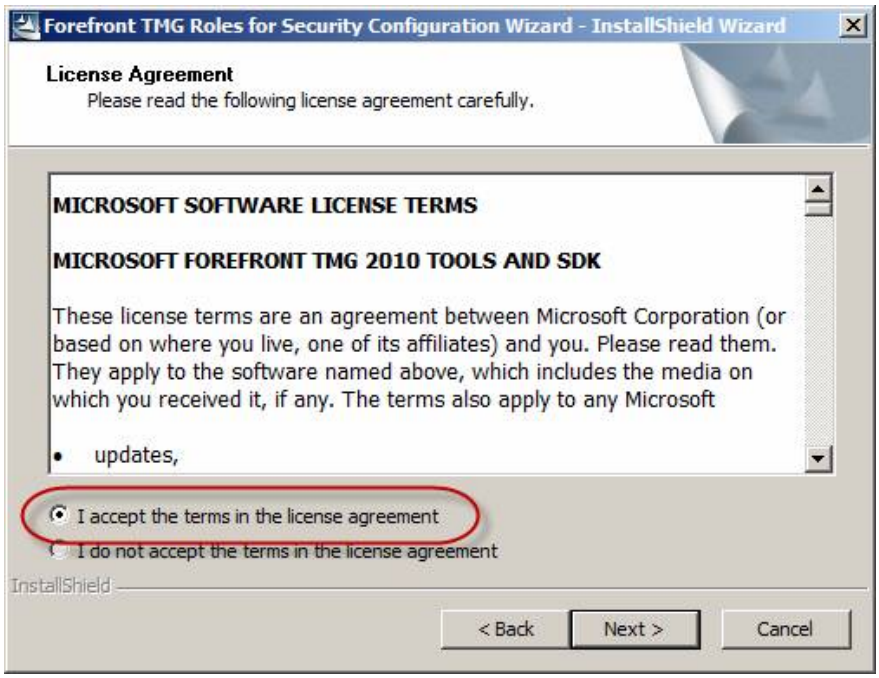

Figure 2

Select the location to save the files.

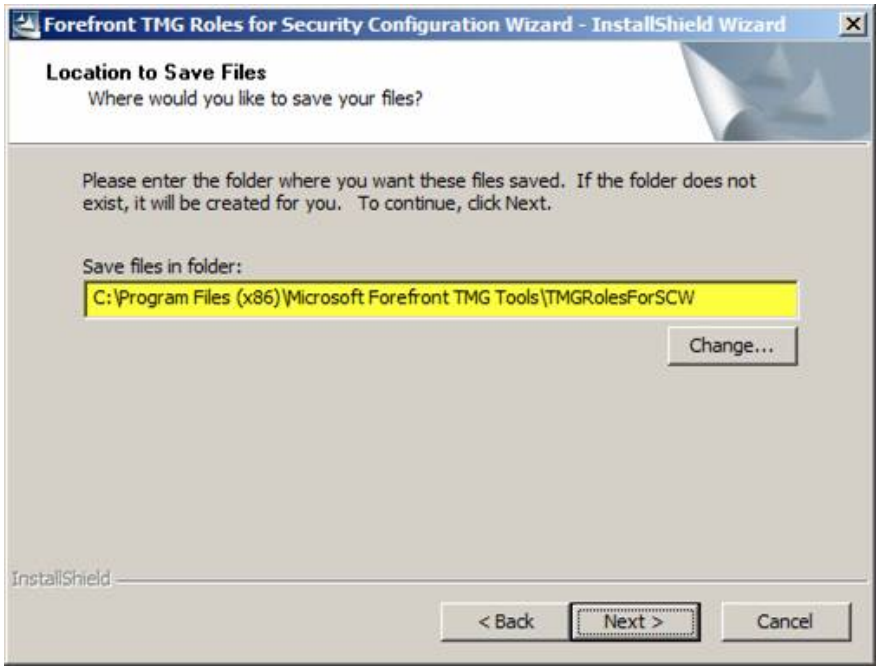

Figure 3

Select **Finish** to complete the installation of Forefront TMG Roles for SCW.

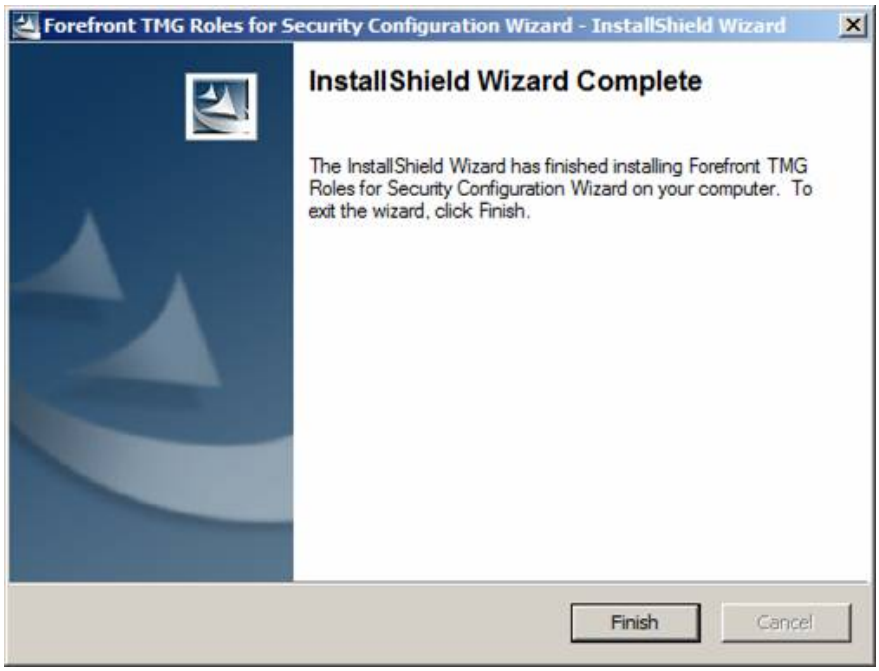

Figure 4

After completing the installation, the next step is to register these new roles with SCW. To register these roles, navigate to the directory you choose to save the files and copy one of the files below to **% systemroot%**

securitymsscwkbs :

- For TMG on Windows Server 2008 SP2, copy scw_tmg_w2k8_sp2.xml
- For TMG on Windows Server 2008 R2, copy scw_tmg_w2k8r2_sp0.xml
- For the TMG EMS on Windows Server 2008 SP2, copy scw_tmgems_w2k8_sp2.xml
- For TMG EMS on Windows Server 2008 R2, copy scw_tmgems_w2k8r2_sp0.xml

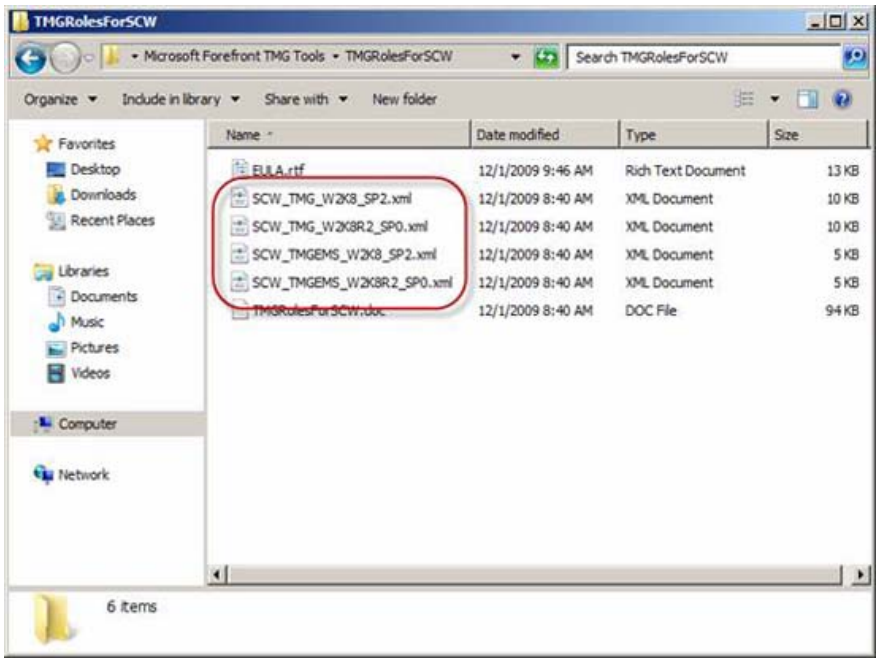

Figure 5

Open the command prompt and navigate to the directory **% systemroot% securitymsscwkbs** , then type one of the following commands:

- For TMG on Windows Server 2008 SP2:
  scwcmd register / kbname: TMG /kbfile:scw_tmg_w2k8_sp2.xml
- For TMG EMS on Windows Server 2008 SP2:
  scwcmd register / kbname: TMG /kbfile:scw_tmgems_w2k8_sp2.xml
- For TMG on Windows Server 2008 R2:
  scwcmd register / kbname: TMG /kbfile:scw_tmg_w2k8r2_sp0.xml
- For TMG EMS on Windows Server 2008 R2:
  scwcmd register / kbname: TMG /kbfile:scw_tmgems_w2k8r2_sp0.xml

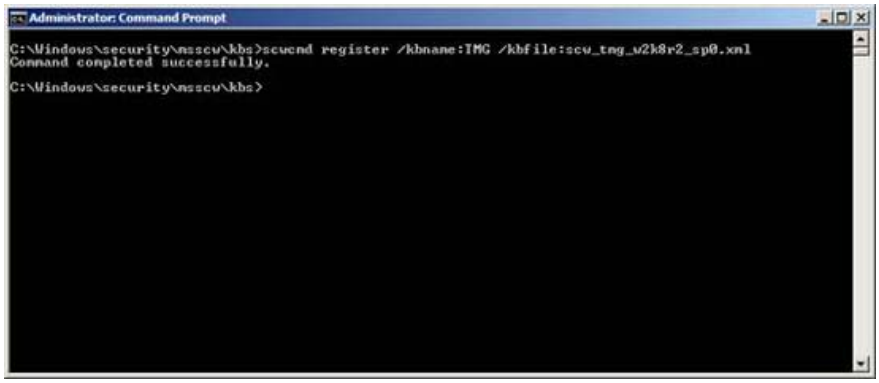

Figure 6

See page 2

Create a security policy with SCW

Open SCW by selecting **Start / Administrative Tools** and clicking the **Security Configuration Wizard** icon **.**

Figure 7

Choose the action you want to perform. For our purposes here, let's select the **Create a new security policy option** . At the end of the policy creation, we can edit, apply, or *roll back* (replace the new ones for the old ones that don't fit) if the policy is needed.

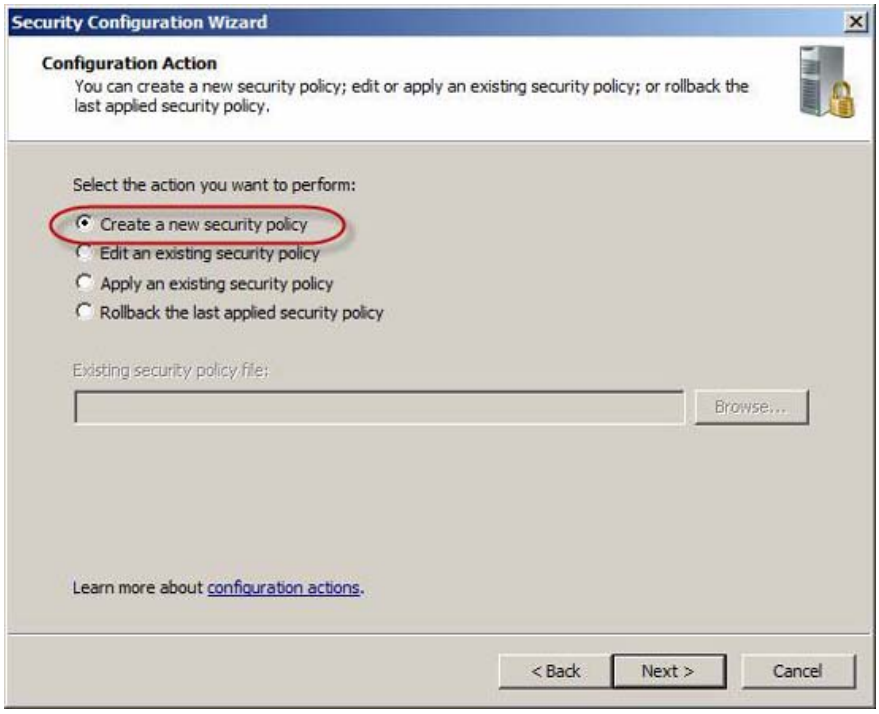

Figure 8

SCW can be used on remote or internal computers. We will configure the policy for the local machine.

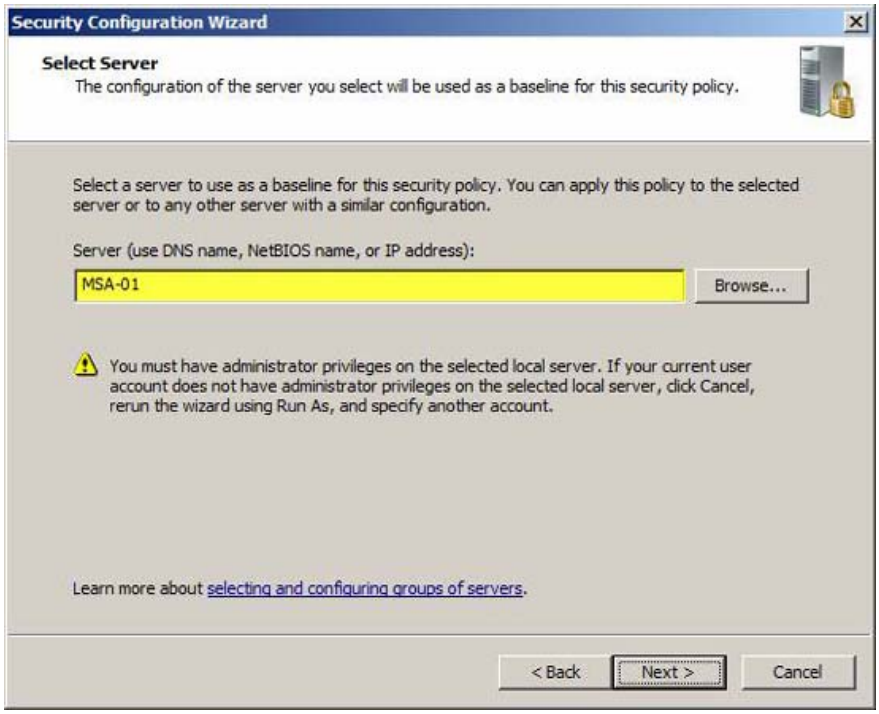

Figure 9

SCW will start the Security Configuration Database process.

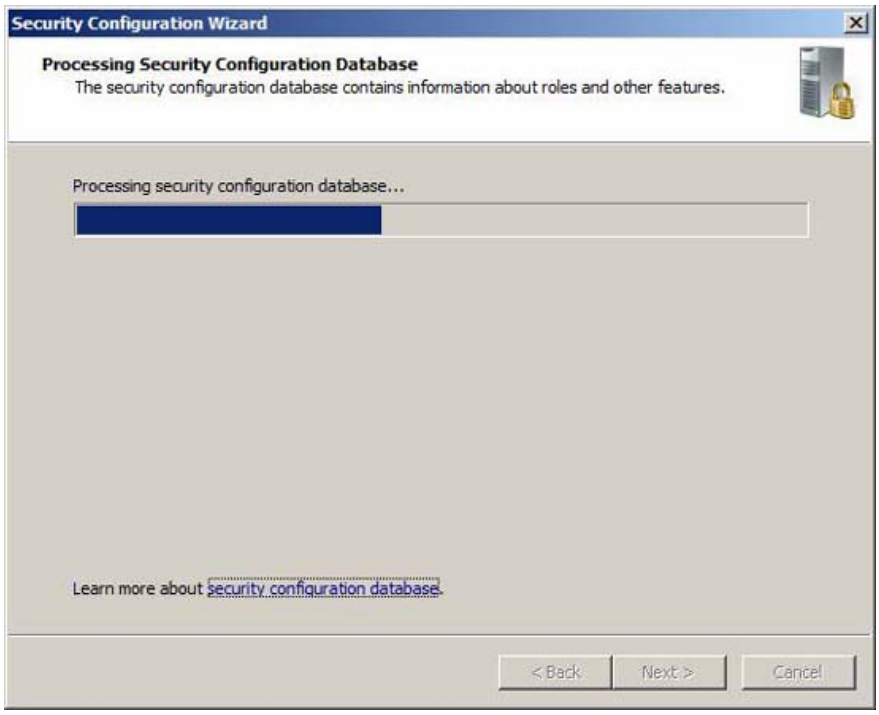

Figure 10

When done, click **View Configuration Database** to confirm that Forefront Threat Management Gateway server role is already in the database.

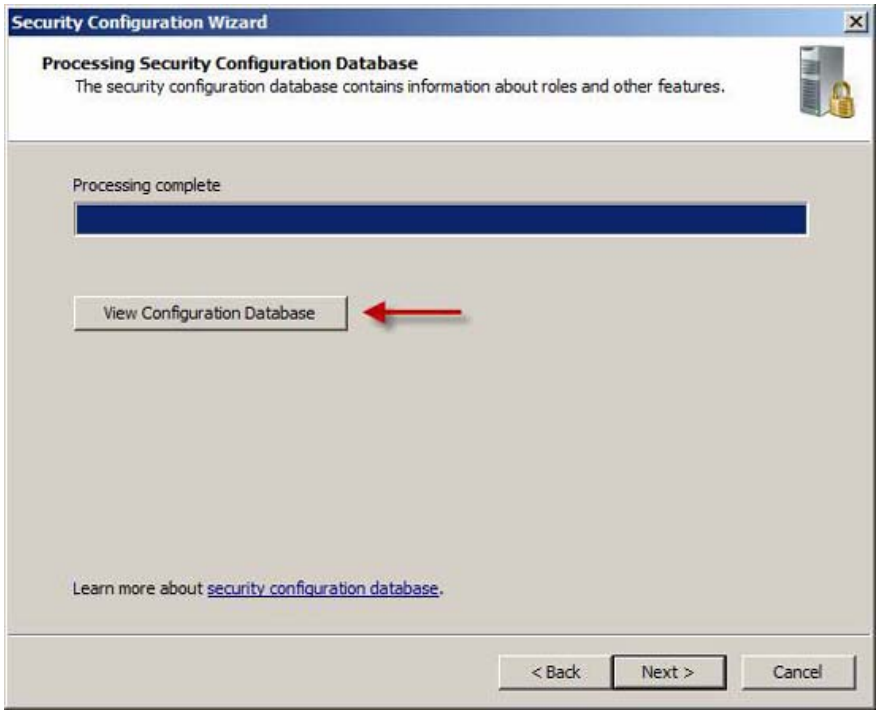

Figure 11

Note : You may receive the security warning below. Then click **Yes** to see the configuration database.

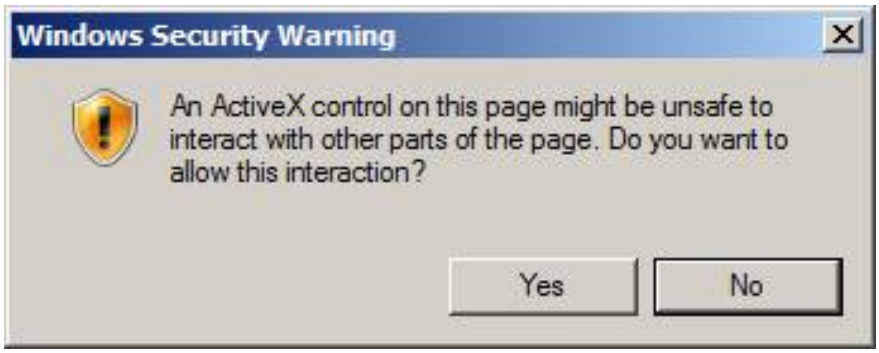

Figure 12

Click the arrow to expand **Server Roles,** and then confirm that **Microsoft Forefront Threat Management Gateway (TMG)** appears in the list. When done, close this window to return to SCW.

Figure 13

See page 3

Roles, features, options and services

SCW will now start configuring the service according to the role

Figure 14

The SCW will configure a security policy based on the roles and features installed on the system. Some installed roles will be selected by default. Click the arrow next to any role to see additional information about that role. Confirm any role selected, then select **Microsoft Forefront Threat Management Gateway (TMG) role.** If your TMG firewall also provides VPN services, select the **Remote access / VPN server** role.

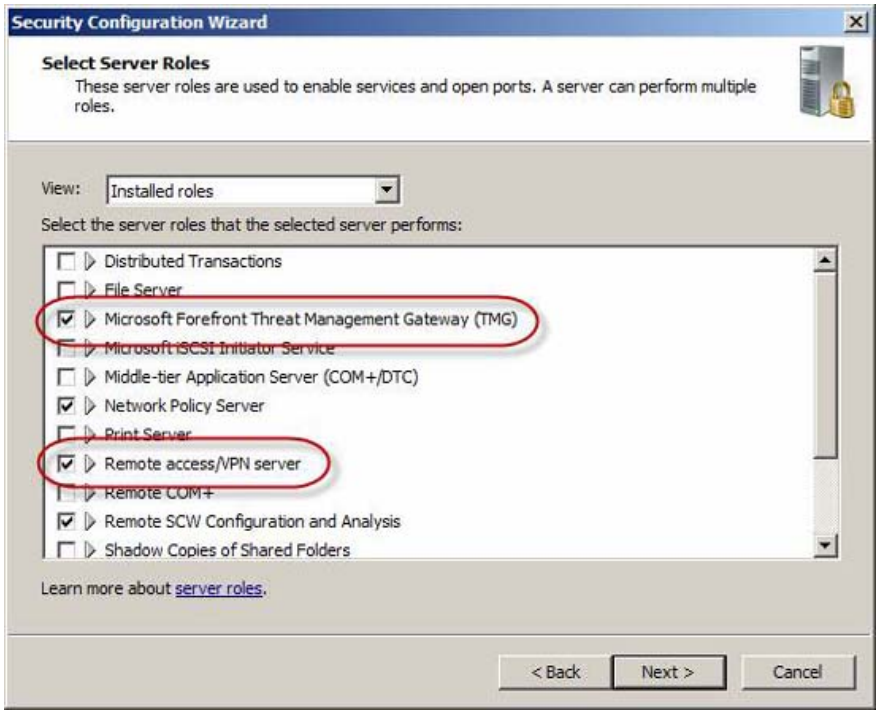

Figure 15

Some installed features will be selected by default. Review selected options and make adjustments as needed. For example, you can disable the **Microsoft Networking Client** or enable **WINS client** completely depending on your security requirements.

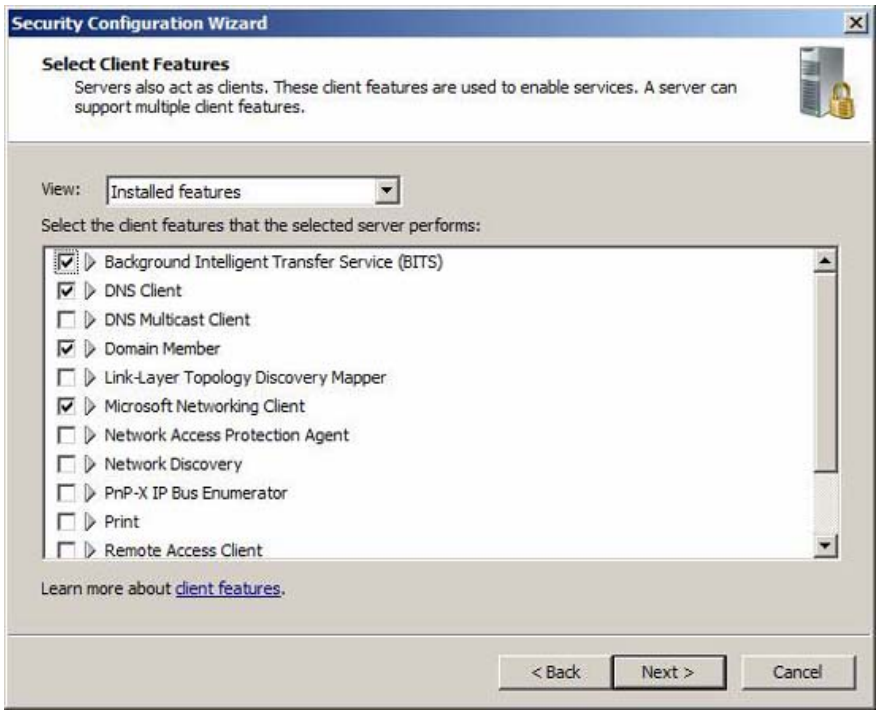

Figure 16

Some pre-installed options are also selected by default. Same as above, review the selected options and adjust them as needed. Review the list carefully because by default there may be features that are not used frequently (such as **Microsoft Fiber Channel Platform Registration Service**). Note that if you want to connect to your TMG firewall using Remote Desktop Services (RDP), select the **Remote Desktop** role (it is not selected by default).

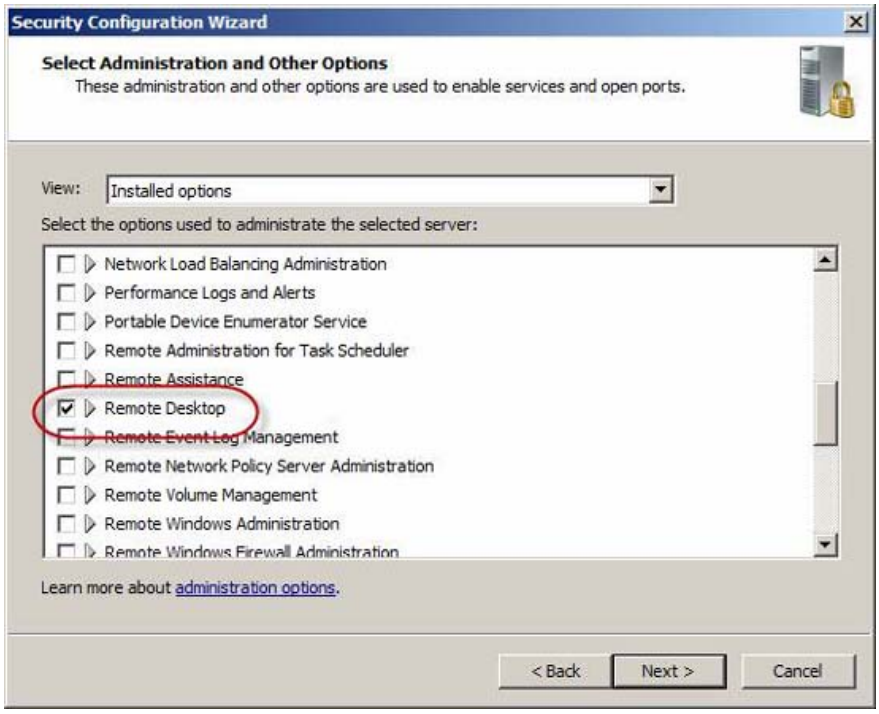

Figure 17

Review the list of additional services and adjust if necessary. The services listed here (selected) will be activated; all other services will be disabled.

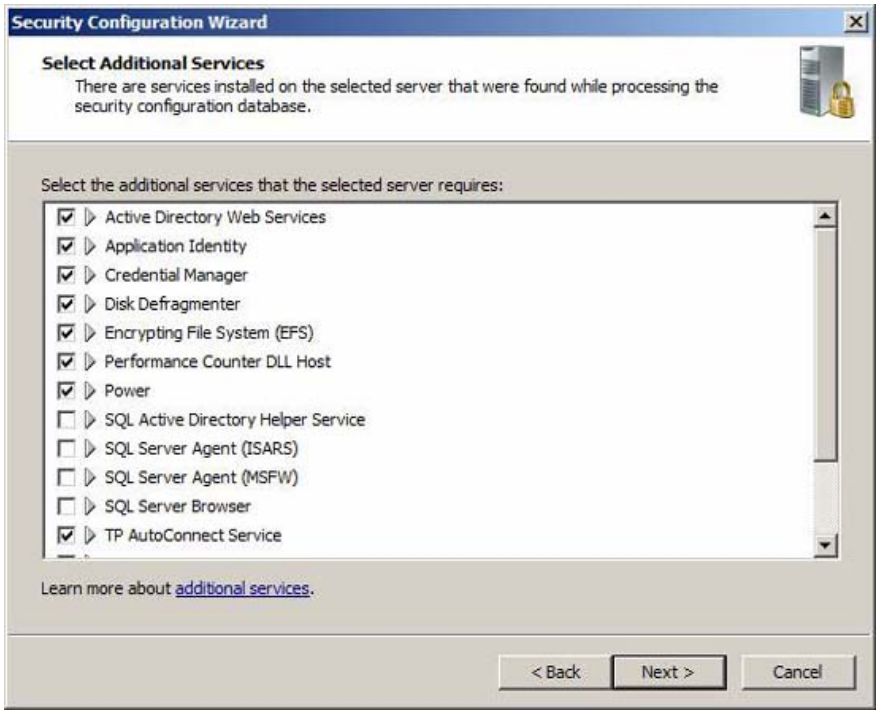

Figure 18

Define how SCW manages unspecified services running on the selected system and not in the security configuration database. Choose the best option for your request. Please do so carefully, because the wrong choice may cause some unexpected consequences.

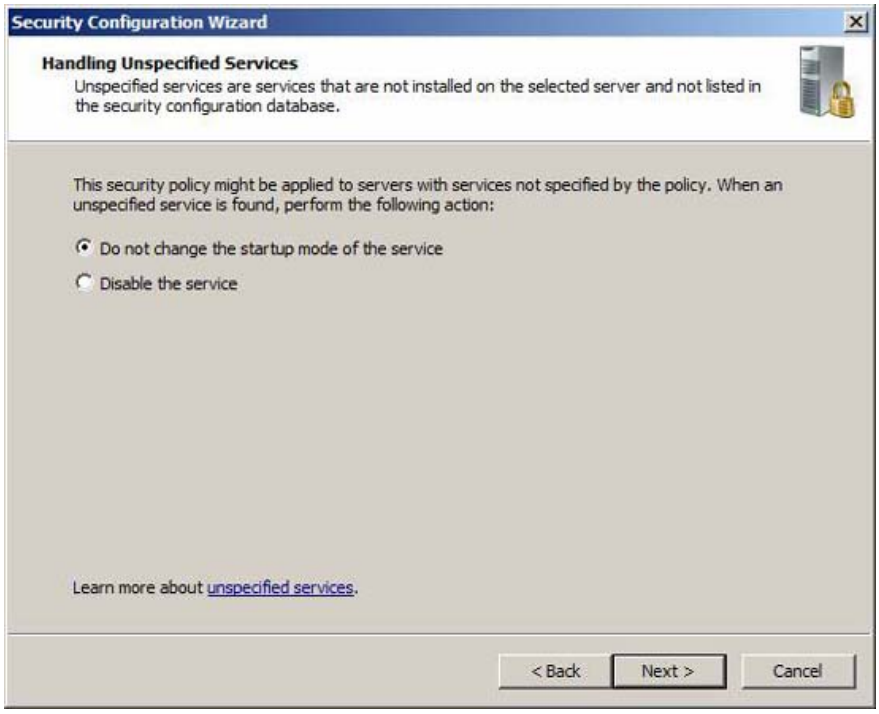

Figure 19

Review the list of changes you have just made for services on the system. If you have selected the option to disable unspecified services, be sure to check the list carefully. Pay attention to the services that the policy will disable in which its current startup mode is automatic. You can sort this list by **Current Startup Mode** by clicking on the column header.

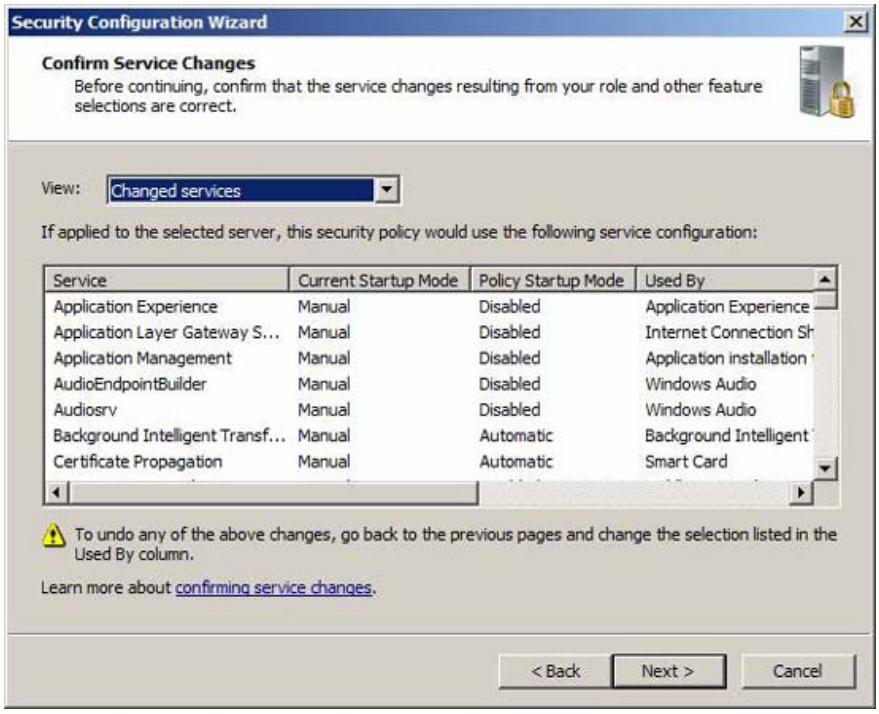

Figure 20

See page 4

Network Security

In this section, the SCW will configure network security settings.

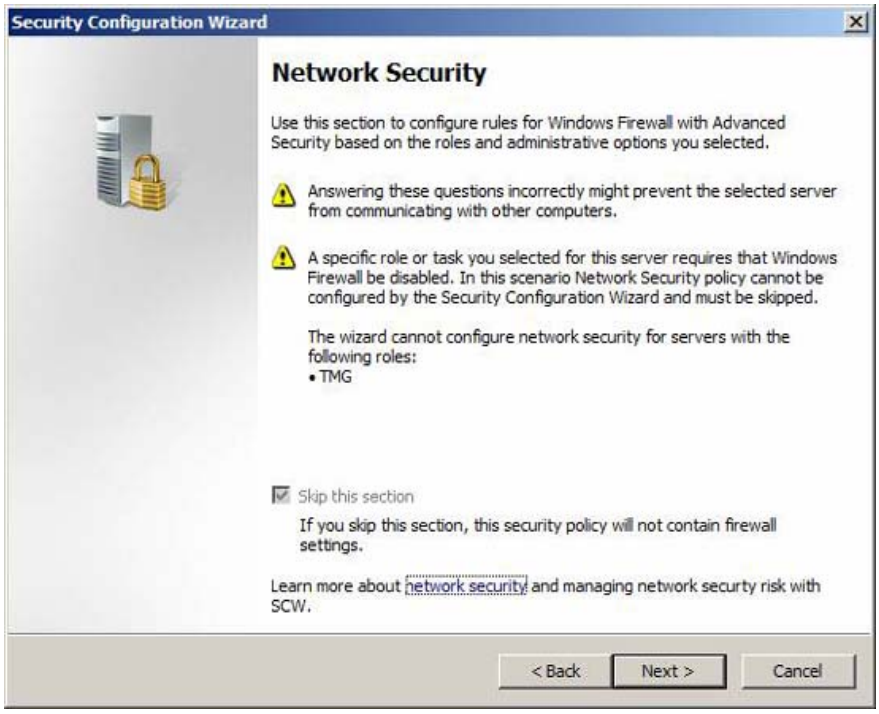

Figure 21

The SCW will configure registry settings that control the protocols used for communicating with other computers. The implementation process is very cautious, because choosing the wrong settings can have unintended consequences. If you are not sure which option to select, safely ignore this option.

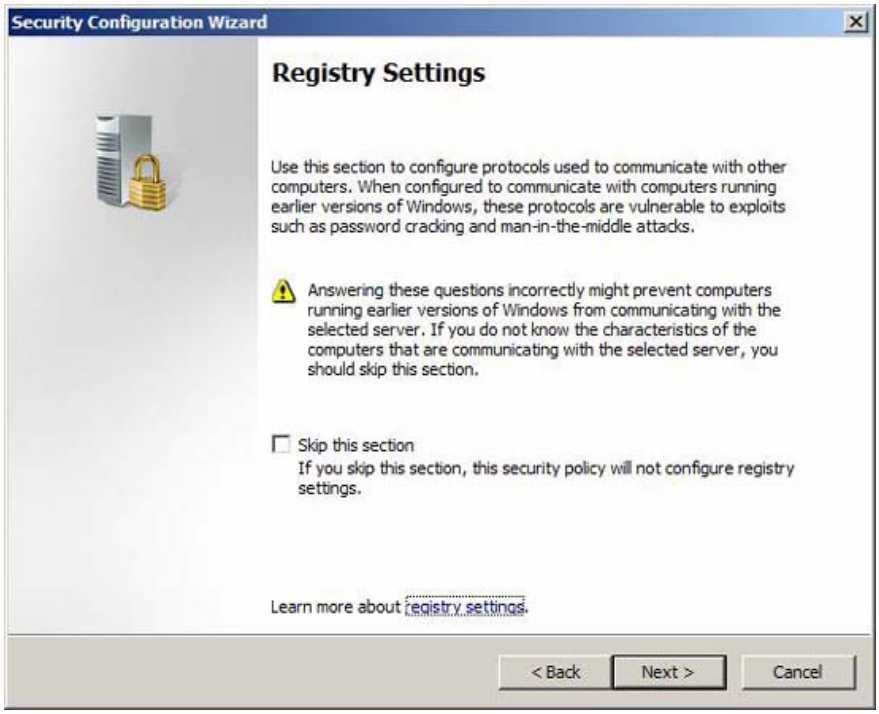

Figure 22

By default, SCW makes assumptions about guest operating systems and the use of TMG systems. Review these options and confirm that they meet your essential requirements.

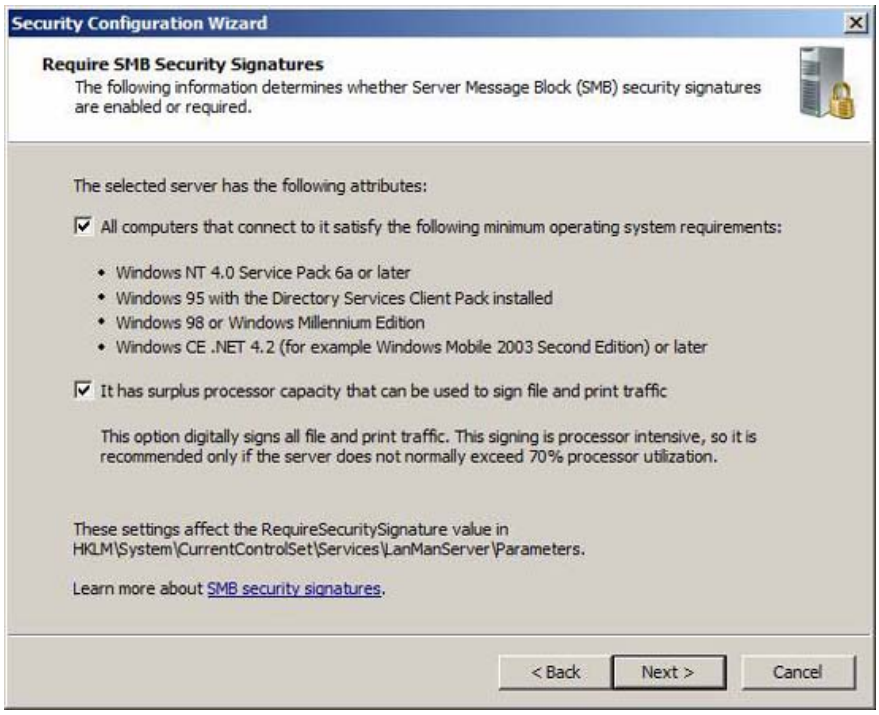

Figure 23

Choose the method of evaluation sent out to meet all your requirements.

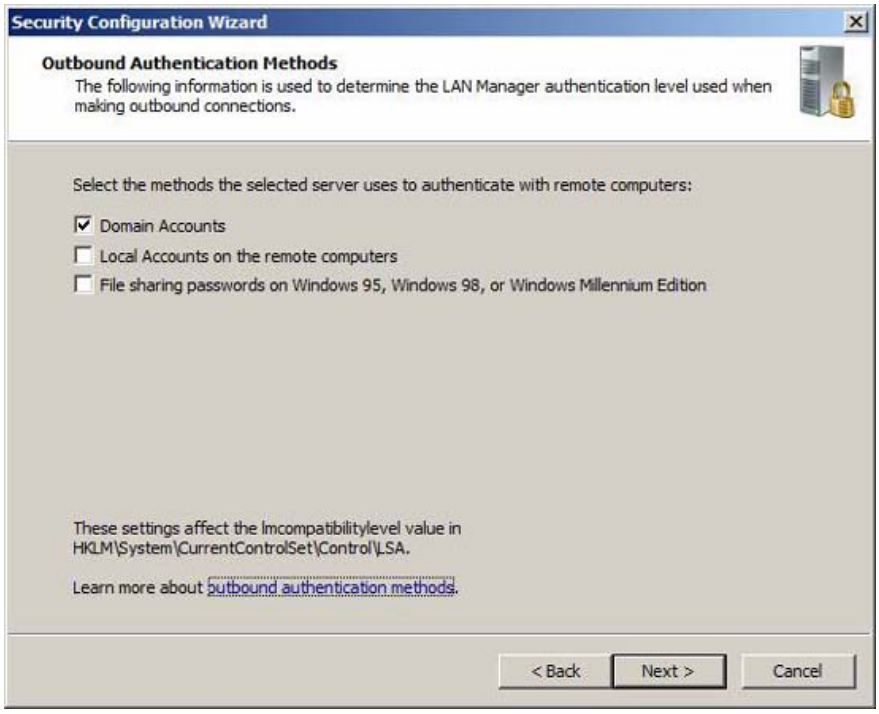

Figure 24

When using domain accounts (highly recommended), you need to confirm that all other computers that the TMG system will communicate with are using a minimum operating system that must also be Windows NT 4.0 SP6A. If your clients synchronize their system clocks with the TMG system, you can choose that option here. This option is not enabled by default because most systems usually synchronize system time with Active Directory domain controllers.

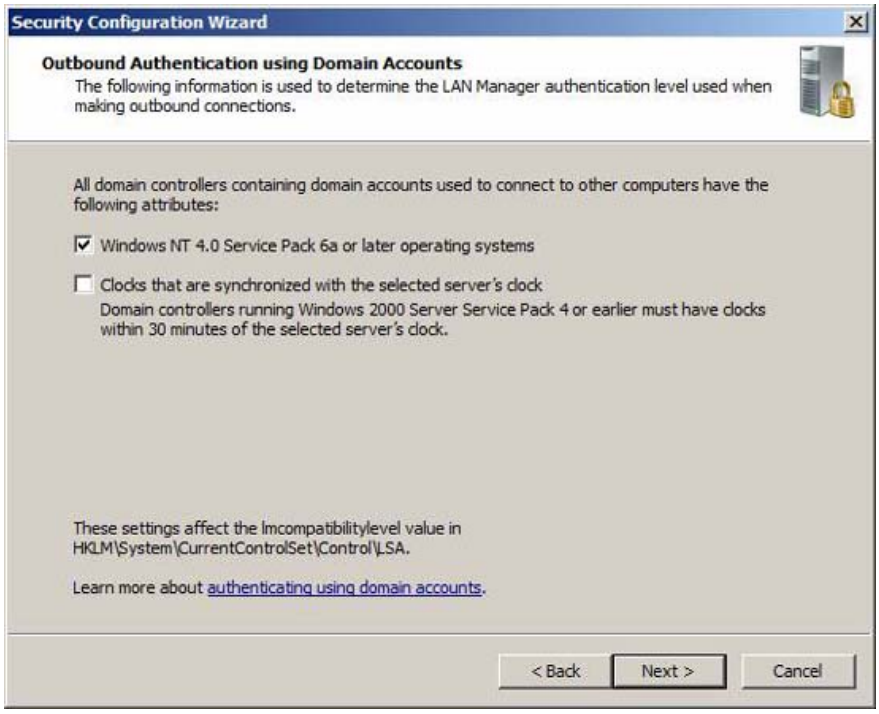

Figure 25

Review the registry settings changes.

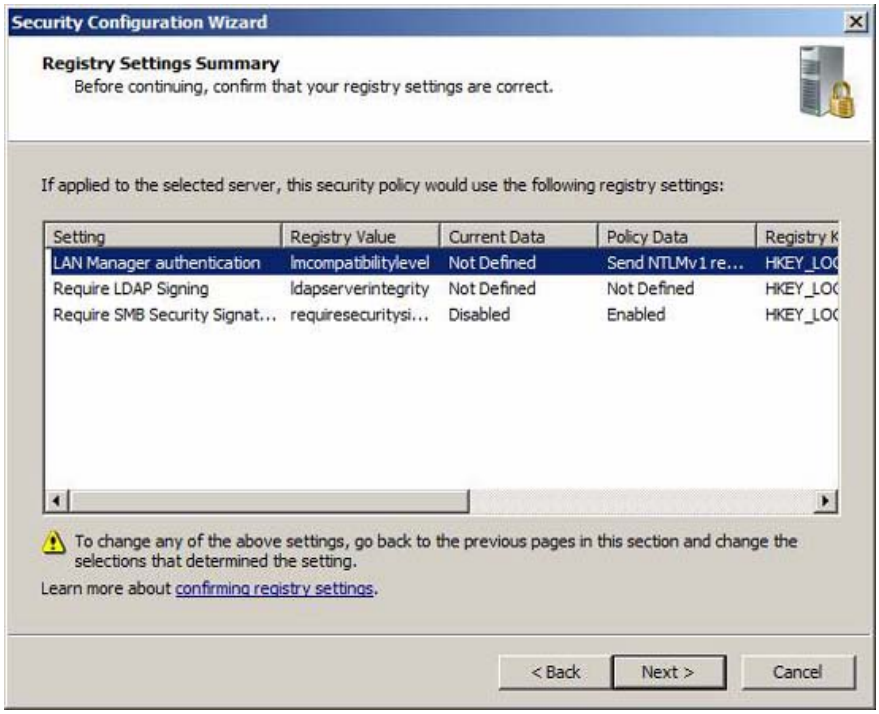

Figure 26

See page 5

Appraisal policy

In this section the SCW will configure the authentication policy. If your authentication policy has been configured to meet all the requirements you need, you can skip this section.

Figure 27

Choose the appraisal option according to your requirements.

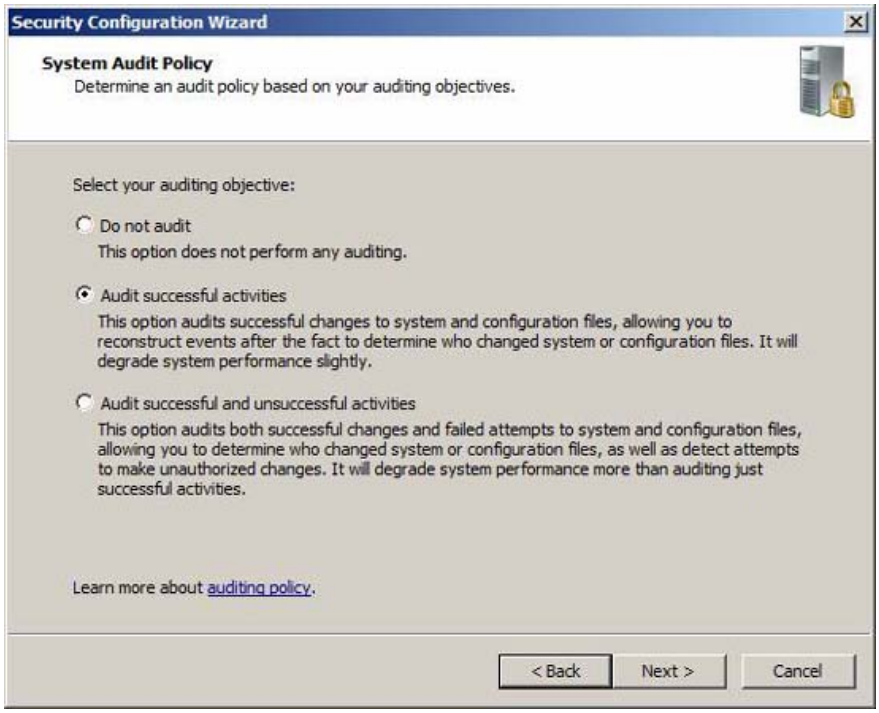

Figure 28

Review the changes you've just made. Note that the option to integrate the **SCWaudit.inf** security template is enabled by default. This secure template will set up System Access Control Lists (SACLS) to help with file system access authentication. The process must be very careful, because when using **SCWaudit.inf,** you cannot remove the use of the SCW rollback option.

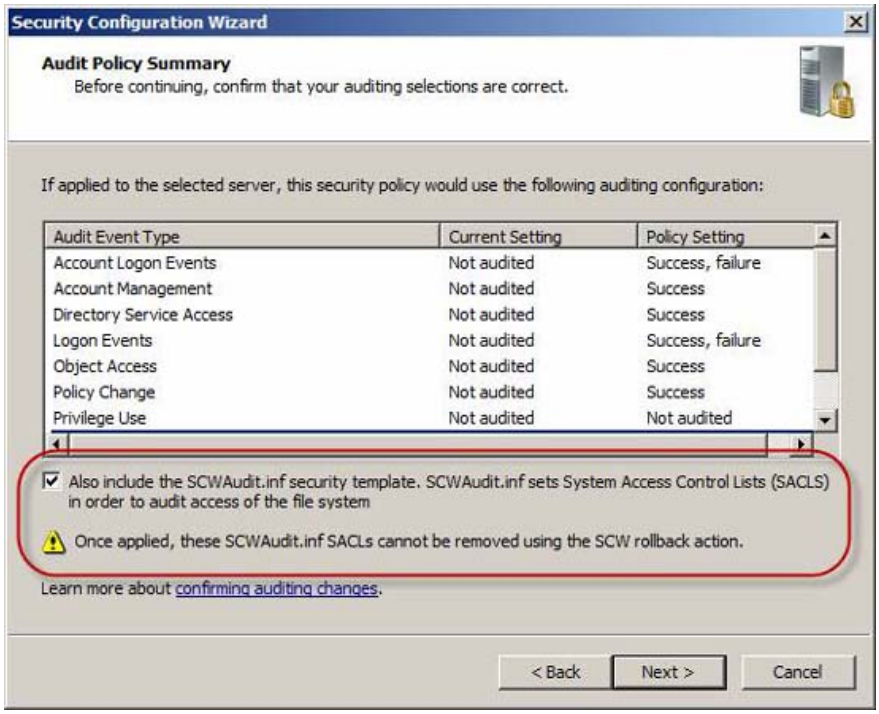

Figure 29

Save privacy policy

Next we need to save the security policy.

Figure 30

Specify the location to save the policy file and include the description (optional but recommended). You can also view security policies or integrate security templates.

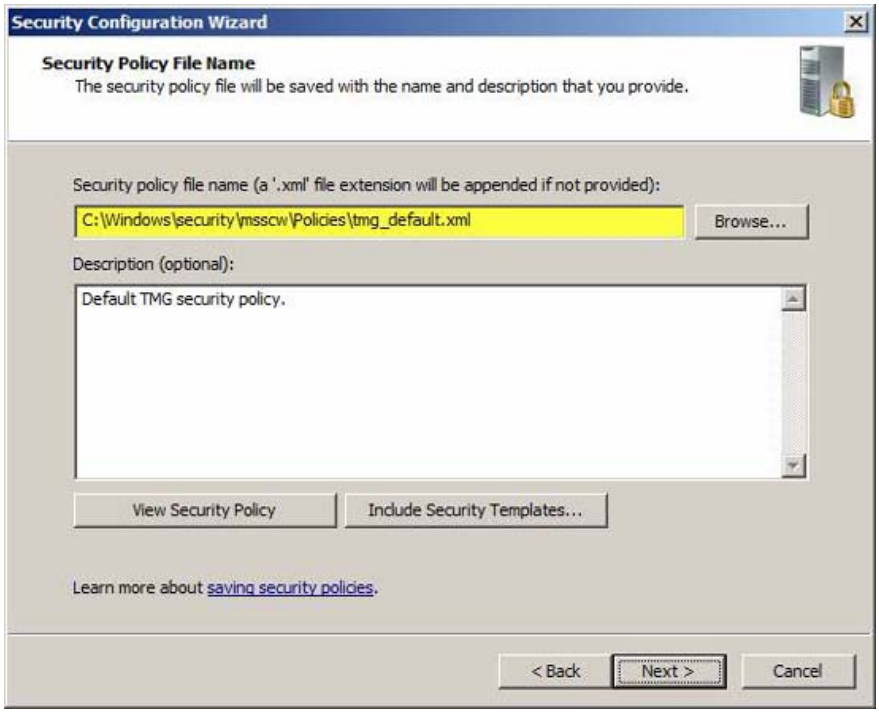

Figure 31

If you are configuring a system, you can choose to use the security policy immediately. If you have multiple TMG firewalls, it's a good idea to deploy a security policy with Active Directory Group Policy. The following section will show you how to do that.

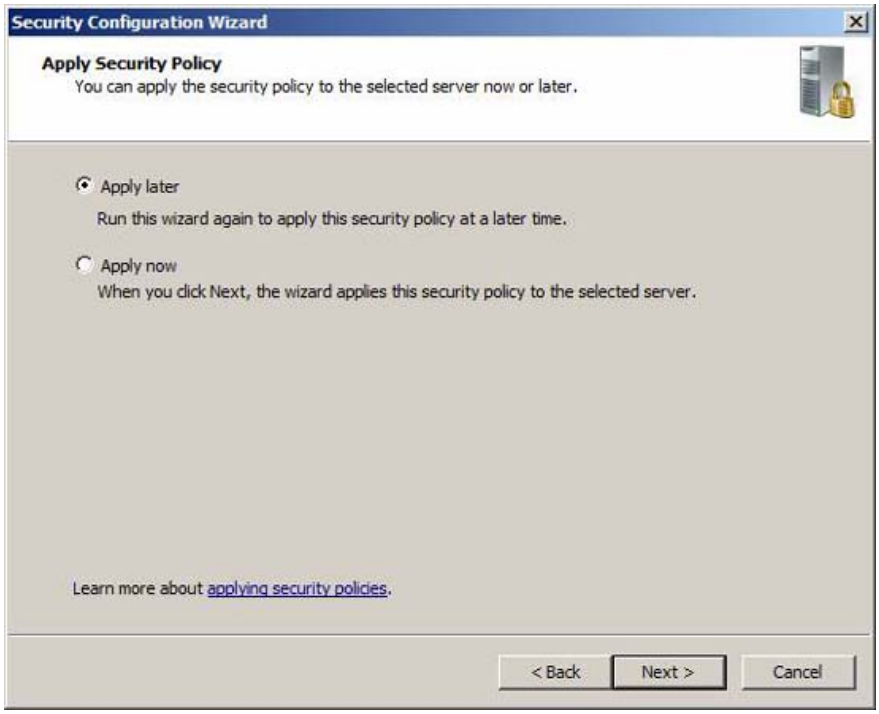

Figure 32

Finish!

Figure 33

Deploy Group Policy

One of the advantages of deploying TMG as a domain member is the ability to manage security configuration using Group Policy. However, SCW is designed to be able to configure and deploy a security policy for only one device at a time (internal or remote). By using the SCW command line tool **scwcmd.exe** we can convert this security policy into a Group Policy Object (GPO), then deploy policies for multiple machines using Active Directory Group Policy. The syntax for that statement is:

scwcmd transform / p: *PathandPolciyFileName* / g: *GPODisplayName*

PathAndPolicyName is a policy created previously, *GPODisplayName* is the name of the Group Policy Object (GPO) and it will appear in the Group Policy Management Console (GPMC).

After the example, open the command prompt and execute the command below:

scwcmd transform /p:tmg_default.xml / g: 'TMG Default'

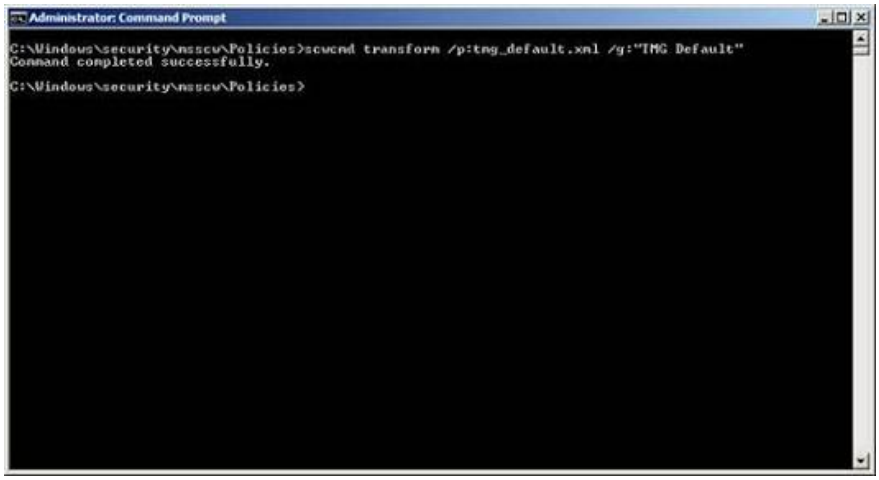

Figure 3 * 4

When the above command is done, open GMPC (**Start / Administrative Tools / Group Policy Management**) and click **Domains** . Open the domain in which the TMG firewall is a member, then open **Group Policy Objects** . Here you will see the new Group Policy object created with the **scwcmd** tool.

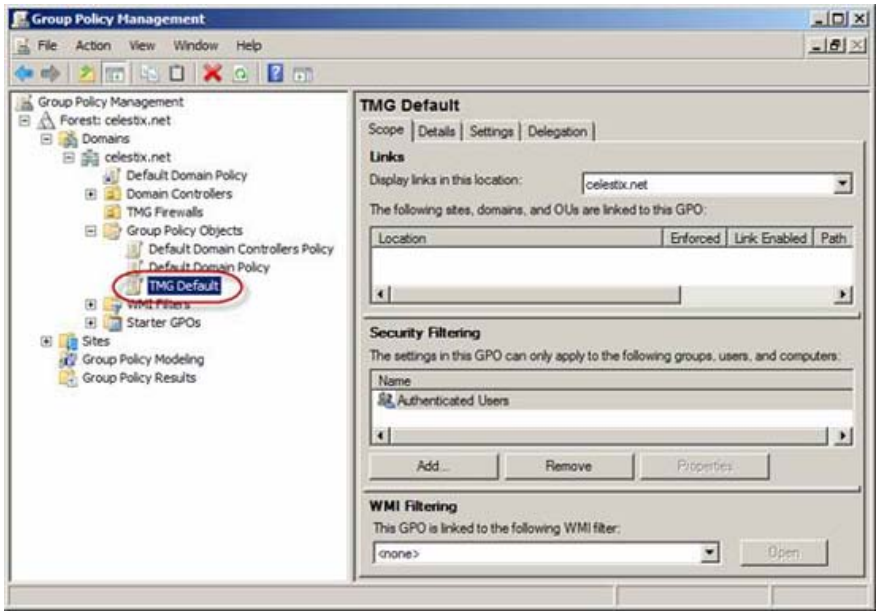

Figure 35

Now you can use this GPO for the Organizational Unit (OU) to integrate your TMG firewall. Ideally, a separate OU should be used for TMG systems to minimize any conflicts that may occur with the application of other GPOs. To use a GPO, select and drag the GPO into the appropriate UO.

Conclude

The correct operating system configuration, service consolidation and attack surface reduction are really necessary for the security and performance of the TMG firewall. Using the Security Configuration Wizard

simplifies and automates this task, allowing administrators to define security policies and apply them in a most consistent way with SCW or Group Policy.