Controlling Internet Access: Introduction to TMG Access Rule - Part 1

In this series, I will show you some of the basics of Access Rules for managing the new TMG firewall.

Network Administration - In this series, I will talk about some of the basics of Access Rules for managing the new TMG firewall .

ISA firewall has a long history of development, the version is gradually upgraded to follow the time and development process.

[#RelatedNews (8) #]

In 2010, the next version of the ISA firewall not only had noticeable new features and functions, it also had a new name - the name ISA was replaced by TMG - **Threat Management Gateway 2010** . This is a big change in perspective and a good signal of efficiency in Microsoft's security development process, Microsoft has completely changed the way software is created and focused on security in all development stage.

The challenge for new TMG firewall settings is to learn the basics. We have spent decades working with ISA and almost every administrator has a deep understanding of the technical details as well as its complex deployment scenarios. However, there are many people who have problems accessing the TMG firewall as well as the way they work. Many new TMG administrators have focused on understanding how to control inbound access (for example, to control access to Exchange and SharePoint). And now they want to know how to control access to outbound connections. That's why we will show you this article, which will focus on the basics of Access Rules.

Learn about Access Rules

Access Rules are used to control access sent from a network protected by the TMG firewall. When you want to allow a computer behind the TMG firewall's control to access another network (including the Internet), you need to create an Access Rule to allow that connection. By default, no Access Rules allow connections through the firewall, so the TMG firewall is a solid brick wall that protects the network. This default closure is a safe configuration, but it also means that if you want to allow traffic through the TMG firewall, you need to understand how Access Rules work and how to create them.

Create an outgoing Access Rule

To begin, we will create a simple outbound Access Rule that allows all users to access the Internet with all protocols. In the next part of this series, we will go into the details of Access Rules and see what dependency issues Access Access has and how you can adjust those dependencies.

Let's start by opening the TMG firewall console and clicking the **Firewall Policy** button in the left pane of the interface, as shown in the figure below.

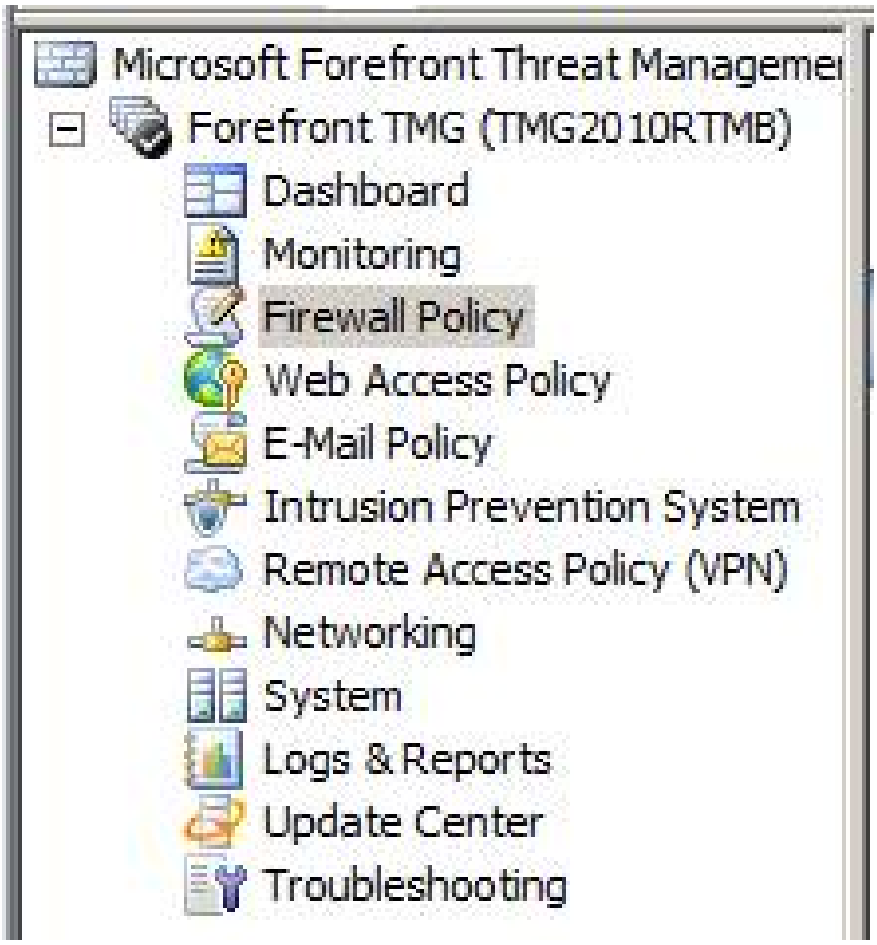

Figure 1

After clicking the **Firewall Policy** button in the left pane, we will click the **Tasks** tab in the right pane of the interface. Here you will see some options, most of them related to creating firewall rules. In this example, we will create an access rule to allow access to be sent through the firewall. Click the **Create Access Rule link** to launch the Access Rule wizard, as shown in the figure below.

Figure 2

On the **Welcome to the New Access Rule Wizard page** , name it in the **Access Rule name** text box. In general, you should place a meaningful name for your Access Rule so that you can scan your firewall policy and know what the rule does, especially knowing the purpose of the rule's purpose. In this example, we will name the rule **All Open 1** . In a production environment, you won't want to create such a rule because this rule will allow all computers to access the Internet and certainly not what you want in a production environment.

Figure 3

On the **Rule Action** page, you will have either **Allow** or **Deny options** for the rule. Note that the default option is Deny, which is a good option in terms of security. We will change the **Deny** status to **Allow** before clicking **Next** to make it become a Allow rule.

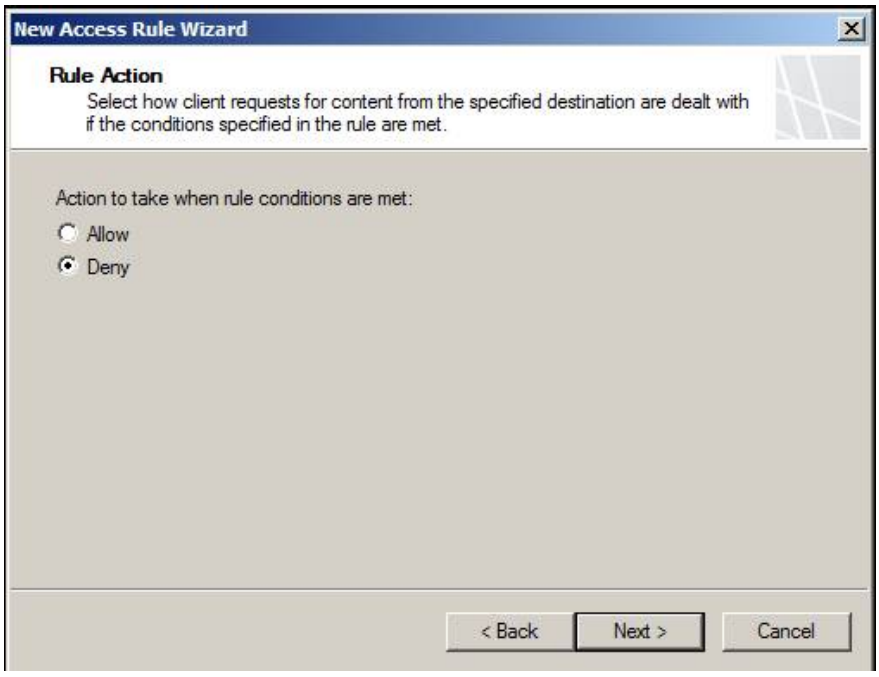

Figure 4

On the **Protocols** page, select the protocols you want to apply to this rule. In the **This rule applies to drop-**down box, you have the following options:

- **All outbound traffic -** Use the option if you want to apply this rule to all protocols.
- **Selected protocols -** Use this option to select certain protocols that you want to apply to this rule. This is a sure option most of you will need.
- **Outbound traffic except except selected -** This option allows you to allow or deny all protocols except for certain protocols that you select.

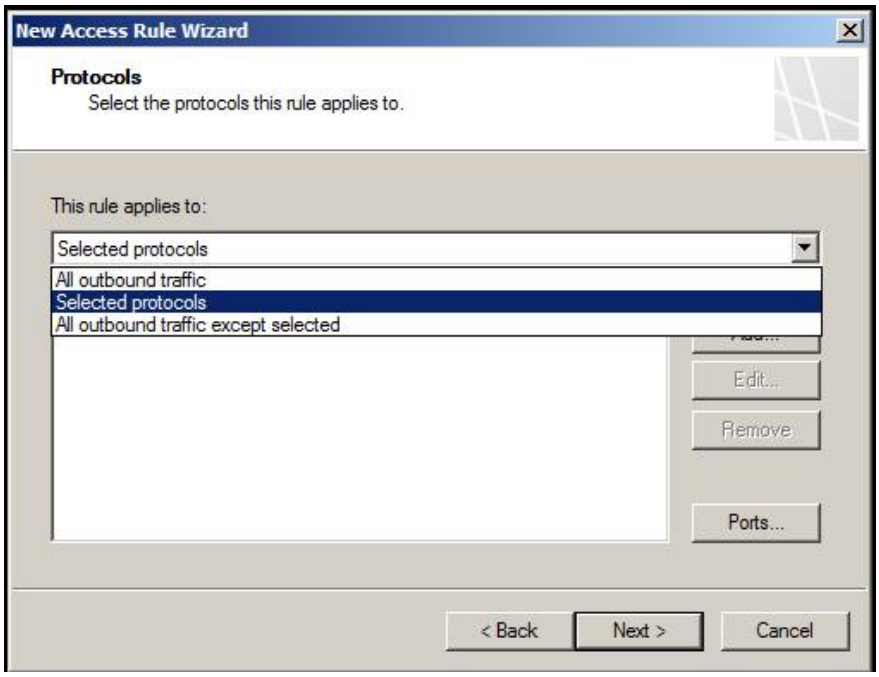

Figure 5

If you select the second or third option, you can click the **Add** button to select the protocols you want to apply to this rule. After clicking the **Add** button, you will see the **Add Protocols** dialog box appear. When you click on a folder in this dialog box, the folder will open and show you a list of protocols. The TMG firewall development team has made it easy to use the separation of protocols in groups to make it easier for you to find the protocols you care about. Double-click the protocols you want to allow, they will appear on the **Protocols** page in the **Protocols** list **.**

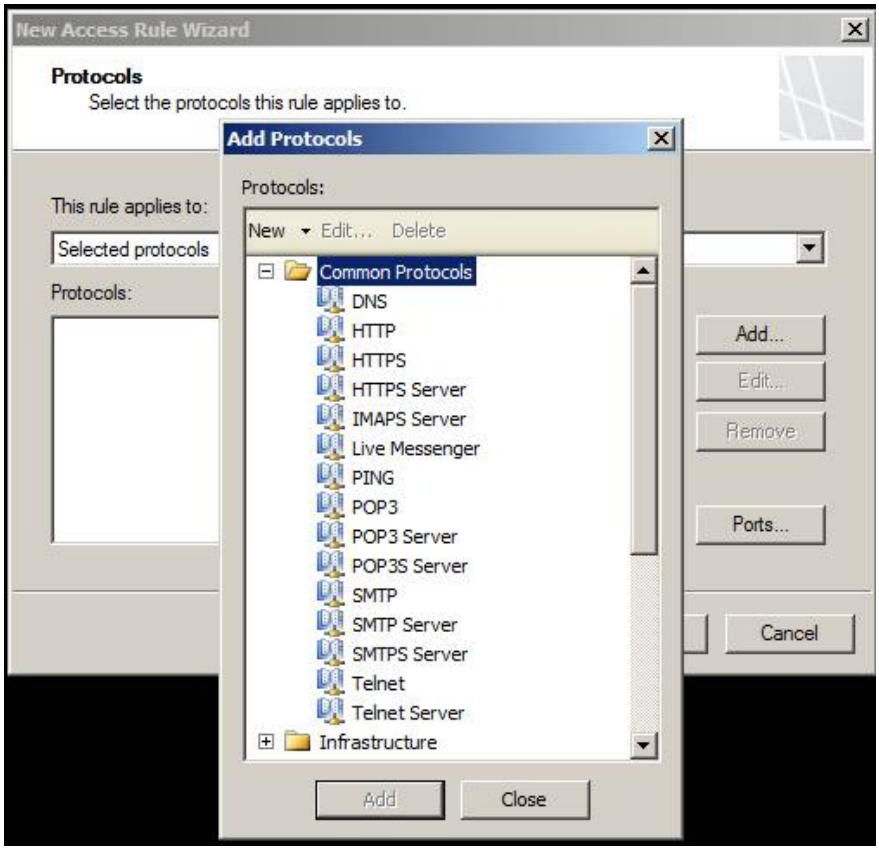

Figure 6

A guest option you have on this page will be revealed when you click the **Source Ports** button **.** Your operation will bring up the **Source Ports** dialog box. Here you can control the allowed source ports for connections that match this rule. Default **Allow traffic from any allowed source port** is selected, however, if you want to block source ports, you can select **Limit access to traffic from this range of source ports** and then enter the values ?? in the **From** and **To** fields. to specify these source ports.

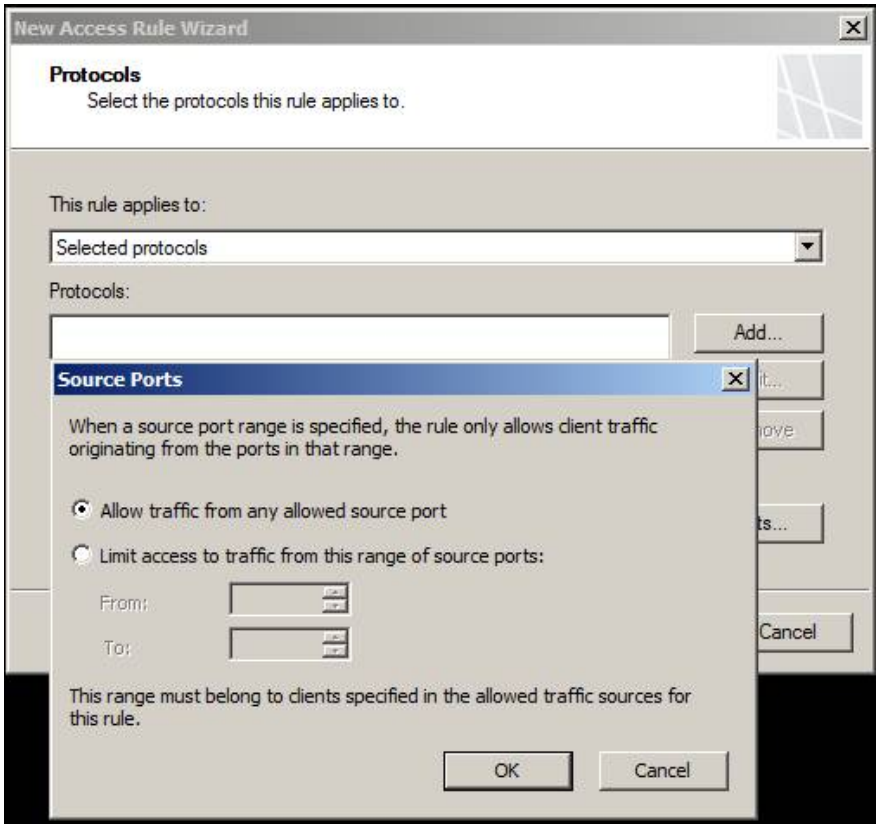

Figure 7

We will not select any source ports at this time but will select the option **All outbound traffic** and then click **Next** .

The next page is **Access Rule Sources.** Here you will choose the location of the computers behind the TMG firewall that you want to apply to this rule. Click the **Add** button and you will see the **Add Network Entities** dialog box. Click the folder that contains the network component that is presenting the source location of the computers on which you want to apply this rule. In this example, we will configure this rule to apply to all computers on the default internal network by clicking the **Networks** folder and then double-clicking on the **Internal** network.

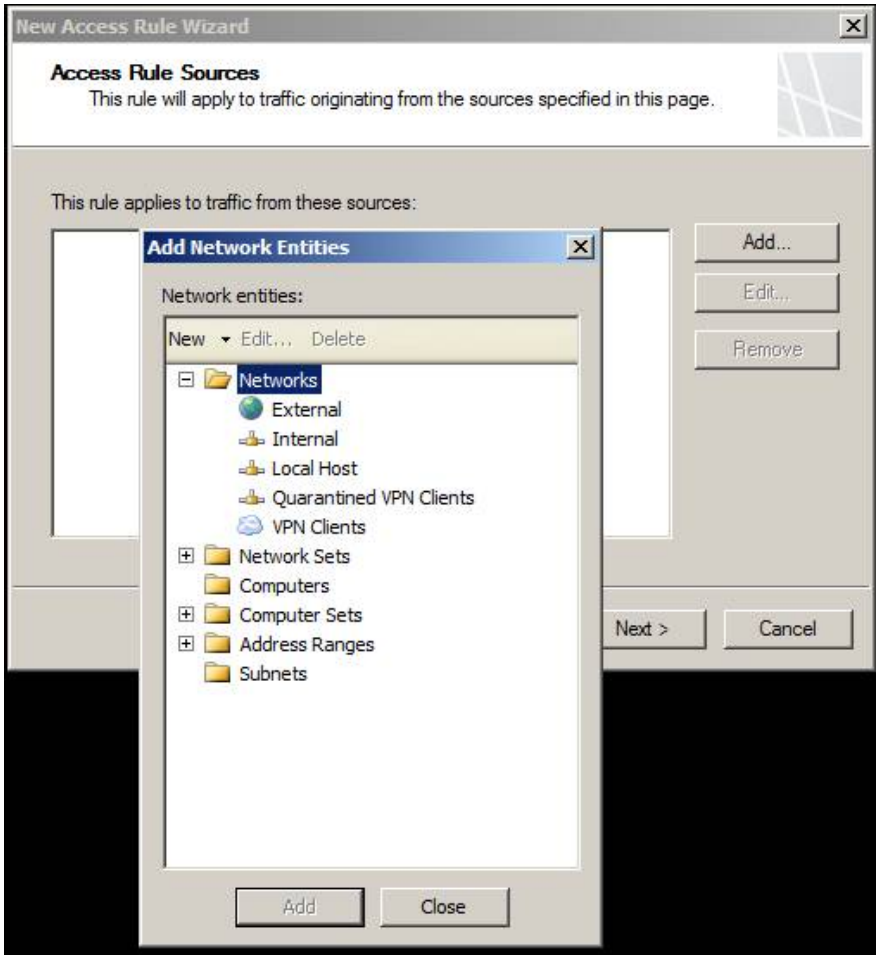

Figure 8

After selecting the source Network as the Internal Network and clicking **Next** , you will see the next page, this is the **Access Rule Destinations** page. Here you set the destination where you want the computers from the previously selected source to access through this rule. The **Access Rule Destinations page** works the same as the previous page, where you click the **Add** button and then in the **Add Network Entities** dialog box **,** click the folder, and then double-click the network component to allow access to this rule. In this example, we will select the default **External** network.

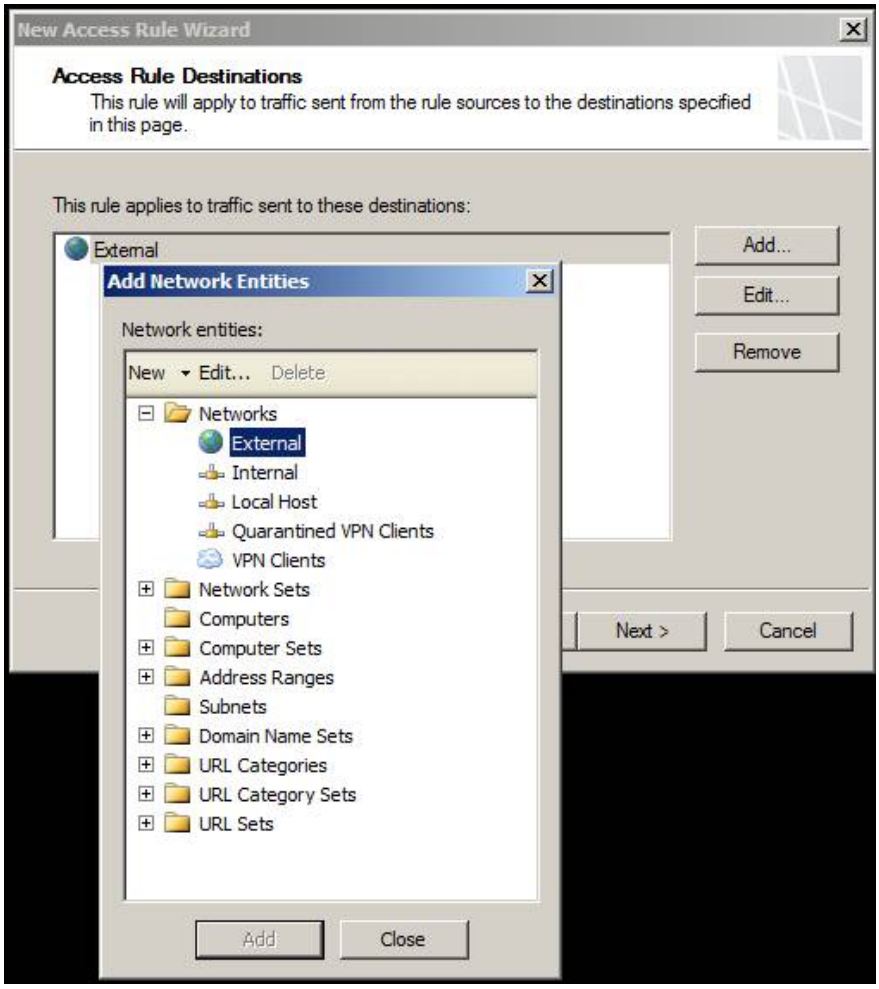

Figure 9

The next page of the wizard is **User Sets** . On this page, you specify the user you want to apply to this rule. By default, Access Rules are applied to all users. For now, defining your 'all users' may not be the same as defining the 'all users' of the TMG firewall. 'All users' doesn't mean your rule will apply to all accounts in your organization, but 'All users' from the TMG firewall perspective means all anonymous users - connections are not received. real. If you click the **Add** button, you can select other users, such as **All Authenticated Users** or **System and Network Service** . You can also create custom user sets based on Active Directory and RADIUS accounts. However, we will mention more about these options in the next section. In this example, we will select the **All Users** option and click **Next** to move to another page.

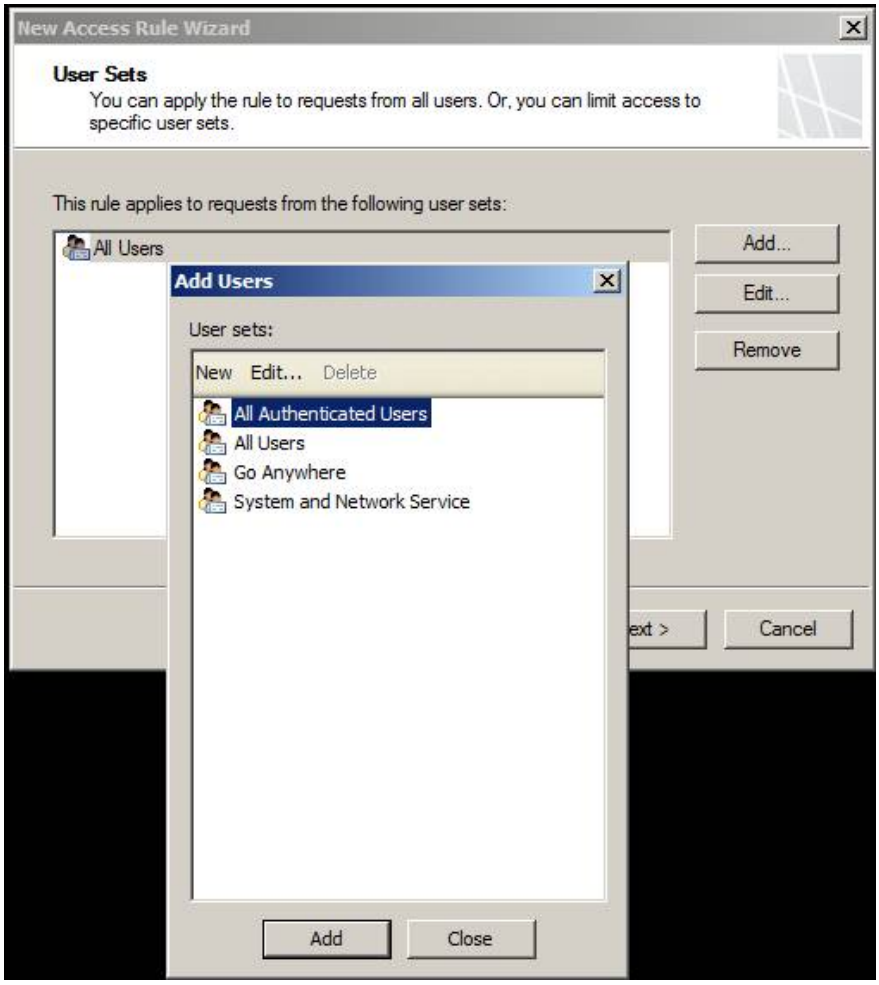

Figure 10

The final page of the wizard is the **Completing the New Access Rule Wizard.** This is the page that allows you to review your settings and then click **Finish** .

Figure 11

After the rule has been created, it will not be valid until you click the **Apply** button at the top of the middle pane in the TMG firewall console. We will click this **Apply** button now.

Figure 12

Other options

After clicking the **Apply** button, the **Configuration Change Description** dialog box will appear. Here you can add a description for the changes you have made to the firewall policy and this description will appear in the change log. The change log is useful when you need to check and find out what you or someone else has done to the firewall policy in case something goes wrong.

Note that you have an option to backup firewall policies by clicking **Export** . This allows you to backup the configuration so that it can be restored to the point before making the change. You also have the option to not display this prompt in the future, but we do not recommend that you choose this option because this is a very useful dialog for you in the future. Now click **Apply** .

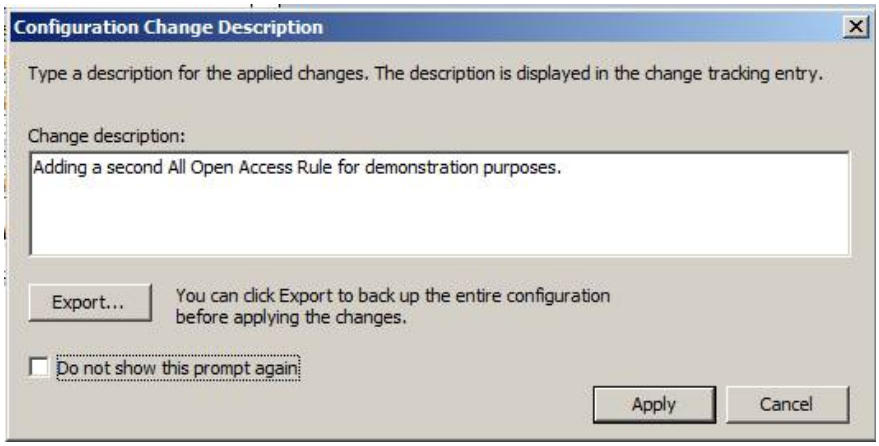

Figure 13

The **Saving Configuration Changes** dialog box appears and tells you that the firewall policy settings have been saved to the configuration repository. Note the text ' **Existing client connections will be reevaluated according to the new configuration. Client connections không h?p l? m?i hi?n th?i ?? xác th?c s? b? b? qua,** means' Existing **client connections will be revalued** according to the new configuration. Client connections that do not correspond to the new policy will be blocked '. This is a new feature in the TMG firewall. With ISA firewall, the new firewall policy is only applied to new connections, not for existing connections. This is a great improvement and is one of the reasons you should upgrade to the latest version of the ISA firewall - named TMG.

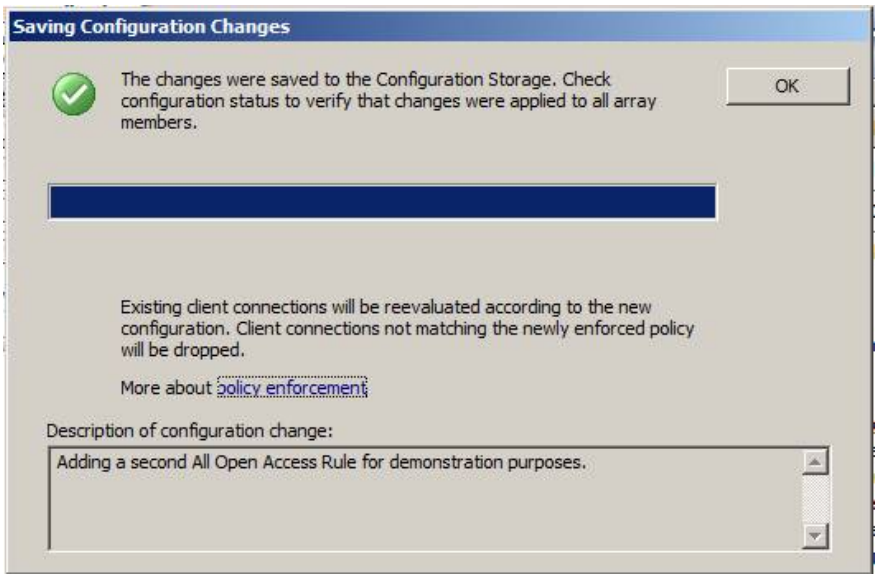

Figure 14

This new rule appears in the firewall's policy list, as you can see in the figure below. The location on the list depends on where you clicked when starting the wizard. However, as we will show you in the next section, you can push this rule up or down in the list.

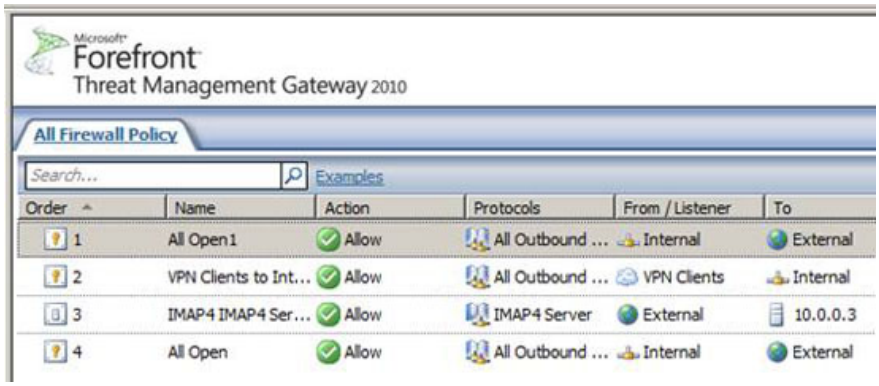

Figure 15

Conclude

In this article, I have shown you some of the basics of Access Rules of the TMG firewall. As you can see, Access Rules are used to control traffic sent from the TMG protected network to other networks. By default, there are no Access Rules and no traffic is possible through the TMG firewall. An Access Rule needs to be set to allow outbound traffic. Access Rules allow you to control traffic, based on a number of factors, such as source location, target location, user, protocols to be used. There are also many other options that have not been revealed in the Access Rule wizard, and we will show you these options in the next section.