Configure One-to-One NAT with TMG 2010

In this tutorial we will show you how to configure a one-to-one NAT Rule for internal hosts.

In this tutorial we will show you how to configure a one-to-one NAT Rule for internal hosts.

Microsoft Forefront Threat Management Gateway (TMG) 2010 has a lot of advanced features like URL filtering, malicious code protection, Network Inspection System (NIS), HTTPS inspections, and ISP attention. However, below these features there are many other important features as well, one of which needs to be introduced is Enhanced NAT (E-NAT).

One-to-One NAT configuration

E-NAT allows you to forward multiple *-to-one* or *one-to-one* IP addresses , such as some existing firewalls (Cisco, Checkpoint, .). However, configuring *one-to-one* NAT in TMG is not simple. If you are familiar with working with Cisco firewalls and Checkpoint, you will definitely want a **NAT rule** tab in the TMG management interface and the **Networking** node **.** However, the problem is that these are really not here.

In TMG, you create a *one-to-one* NAT Rule by creating a **Network Rule** . Suppose we want to forward all traffic coming from an internal host to an IP address assigned to the external network interface of the TMG firewall (not the default IP address for the interface). To do so, open the TMG console and select the **Networking** button in the navigation menu. Select the **Network Rules** tab in the central control window, then click **Create a Network Rule** in the **Tasks** panel. Name the description for the Rule and select **Next** .

Figure 1

Specify the source of the traffic you want to forward. In this example, we selected a separate server, but you can select networks, a set of networks, a set of computers, a range of addresses, and subnets. This allows us to have high flexibility when establishing NAT relationships in TMG.

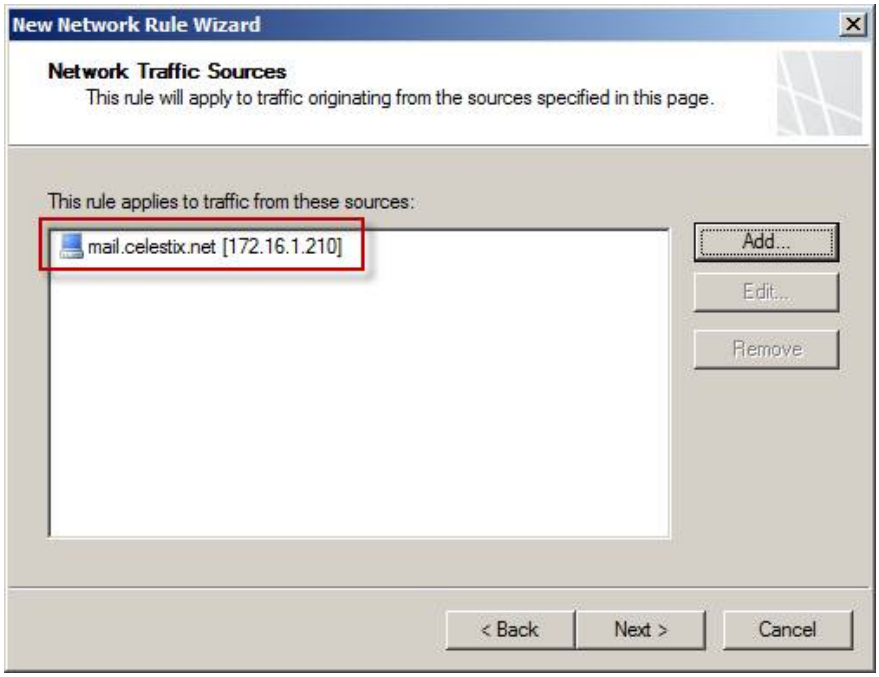

Figure 2

Specify the destination that you want to apply this rule to. In our example, we chose a network outside of External because we want to forward traffic sent from the server using this rule. Here you can choose from a variety of options, which also allow you to have fairly fine-grained control over address forwarding.

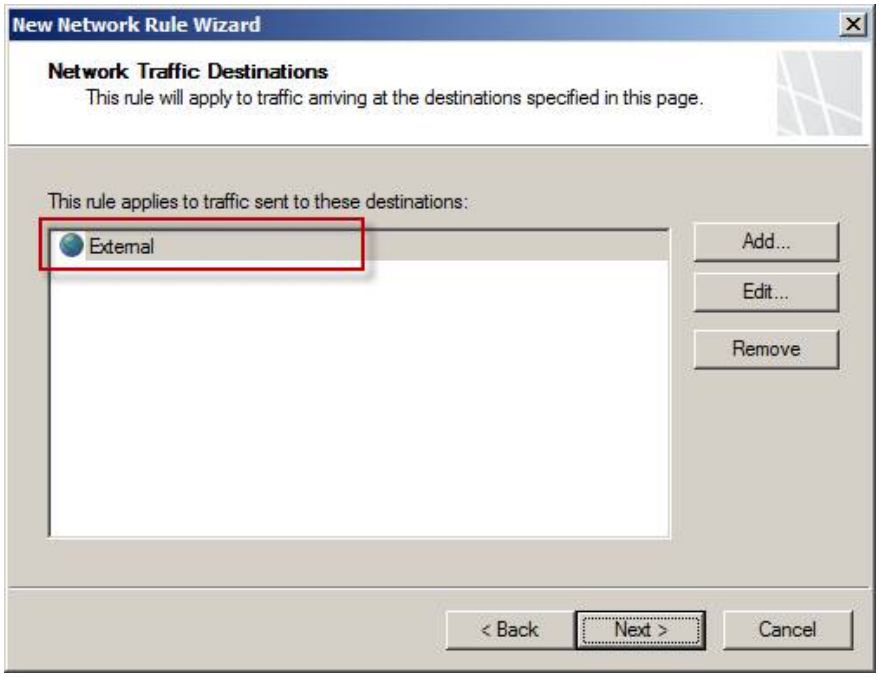

Figure 3

Select the option **Network Address Translation (NAT).**

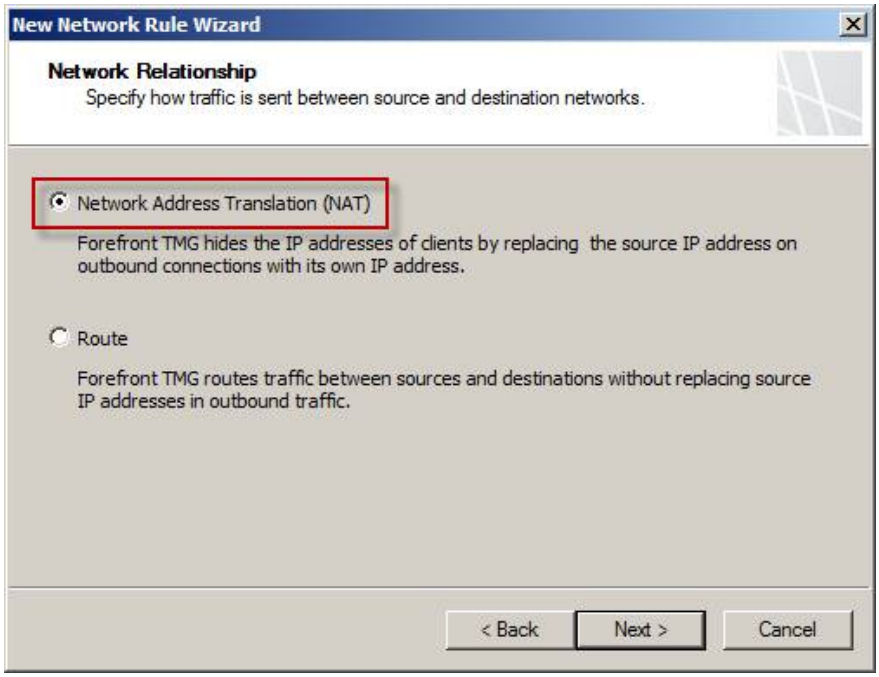

Figure 4

Select the **Use the specified IP address** option and select the IP address from the available list.

Note:

These IP addresses must be assigned to the network interface first to create the rule, otherwise they will not appear in this list.

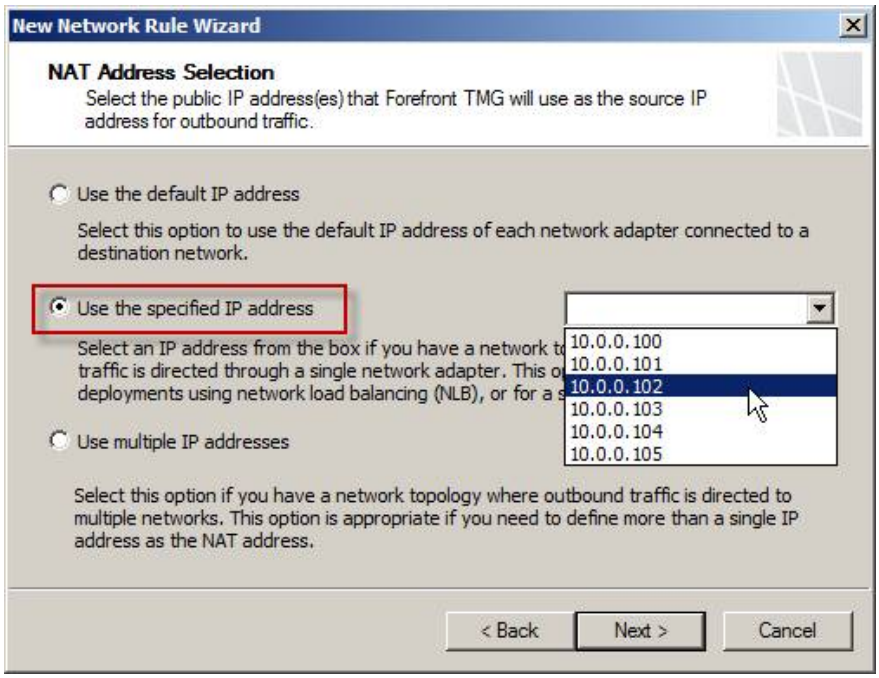

Figure 5

You can also choose the **Use multiple IP addresses** option **,** which allows you to select additional IP addresses for the rule (which makes it useful for business arrays when NLB is not enabled).

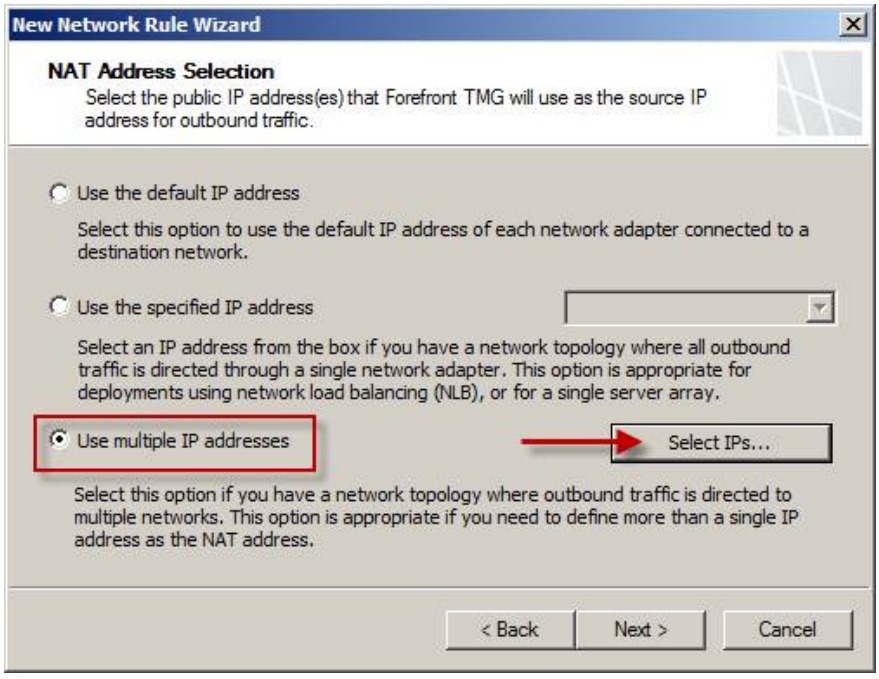

Figure 6

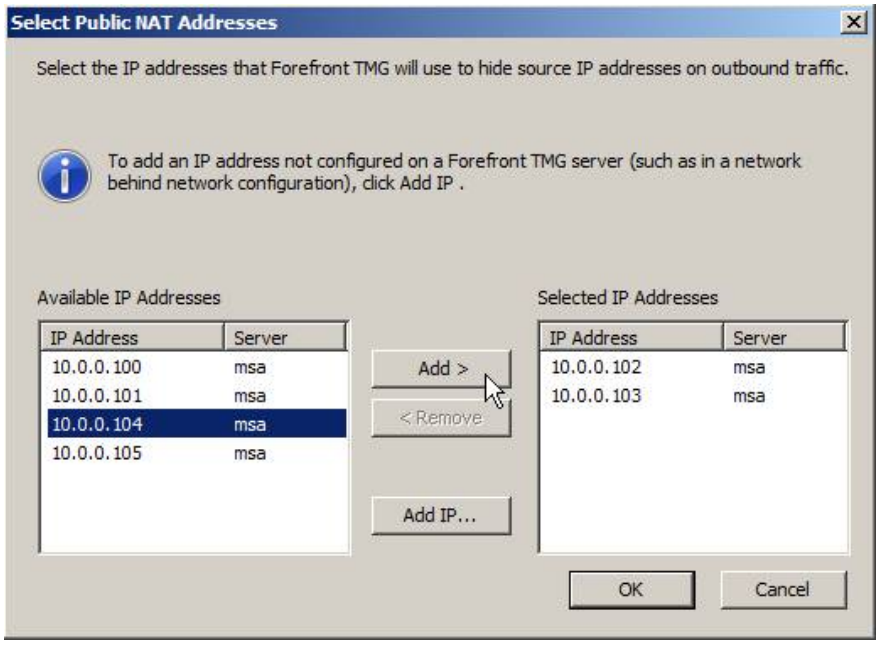

Figure 7

Another important thing you need to know is network rules, like firewall policy rules, they are processed in order. To work properly, more specific rules need to precede other rules. In the example in the article, the specific rule here is defining a NAT relationship between the entire network inside Internal (with the host being one of the members) and the network outside External. After the wizard is complete and before applying the configuration, make sure that this new network rule must appear before the Internet Access rule.

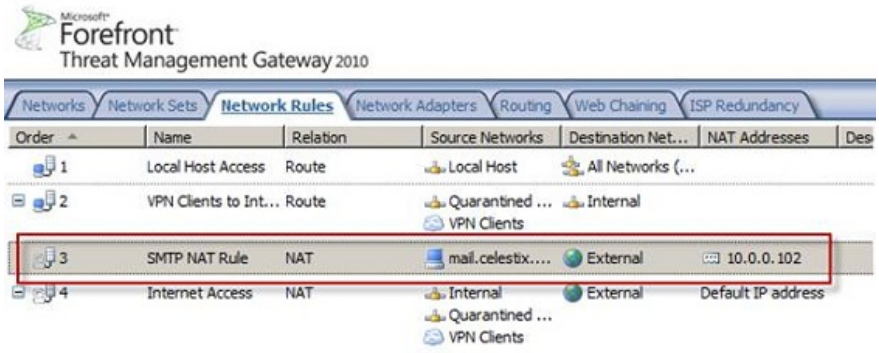

Figure 8

Once configured, the traffic generated from the mail.celestix.net host intended for the network outside the External will match rule number 3, in this rule the network relationship is intended to be NAT, the NAT address is The definition is obviously 10.0.0.2

E-NAT and ISP backup

When the -NAT configuration on the TMG firewall is configured to use a backup ISP (ISP-R), address forwarding may work unexpectedly. When configured, E-NAT rules take precedence and override routing decisions created by ISP-R. Be sure to have a careful plan when implementing both of these techniques.