# Microsoft Forefront TMG – FTP and FTP Server publishing

http://www.isaserver.org/articles-tutorials/configuration-security/Microsoft-Forefront-TMG-FTP-and-FTP-Server-publishing.html

## Contents



How to allow FTP server traffic through TMG Server for outbound connections through Firewall rules and for incoming connections through TMG server publishing rules.

## Introduction

In this article, I will you show you ways to allow FTP server traffic through TMG server for outbound connections through Firewall rules and for incoming connections through TMG server publishing rules. We will also cover some special considerations with FTP in Forefront TMG.

## Let's begin

**Note:**
Keep in mind that the information in this article is based on a release candidate version of Microsoft Forefront TMG and is subject to change.

A few months ago, Microsoft released RC 1 (Release Candidate) of Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exciting features.

One of the new features of Forefront TMG is its ability to allow FTP server traffic through the Firewall in both directions. It does this in the form of Firewall access rules for outbound FTP access and with server publishing rules for inbound FTP access through a published FTP Server. This server is located in your internal network or a perimeter network, also known as a DMZ (if you are not using public IP addresses for the FTP Server in the DMZ).

First, I will show you the steps you will need to follow in order to create a Firewall rule which will allow FTP access for outgoing connections through TMG.

## FTP access rule

Create a new access rule which allows the FTP protocol for your clients. If you want to allow FTP access for your clients, the clients must be Secure NAT or TMG clients, also known as the Firewall client in previous versions of Forefront TMG.

**Please note:**
If you are using the Web proxy client, you should note that through this type of client only FTP read-only access is possible and you cannot use a classic FTP client for FTP access, only a web browser FTP access is possible with some limitations.

The following picture shows a FTP access rule.


**Figure 1:** FTP access rule

A well-known pitfall beginning with ISA Server 2004 is, that by default, after the FTP access rule has been created, the rule only allows FTP read-only access for security purposes in order to prevent users from uploading confidential data outside the organization without permission. If you want to enable FTP uploads you have to right click on the FTP access rule, and then click Configure FTP.


**Figure 2:** Configure FTP

All you have to do is remove the read only flag, wait for the new FTP connection to be established, and the users get all the necessary permissions to carry out FTP uploads.

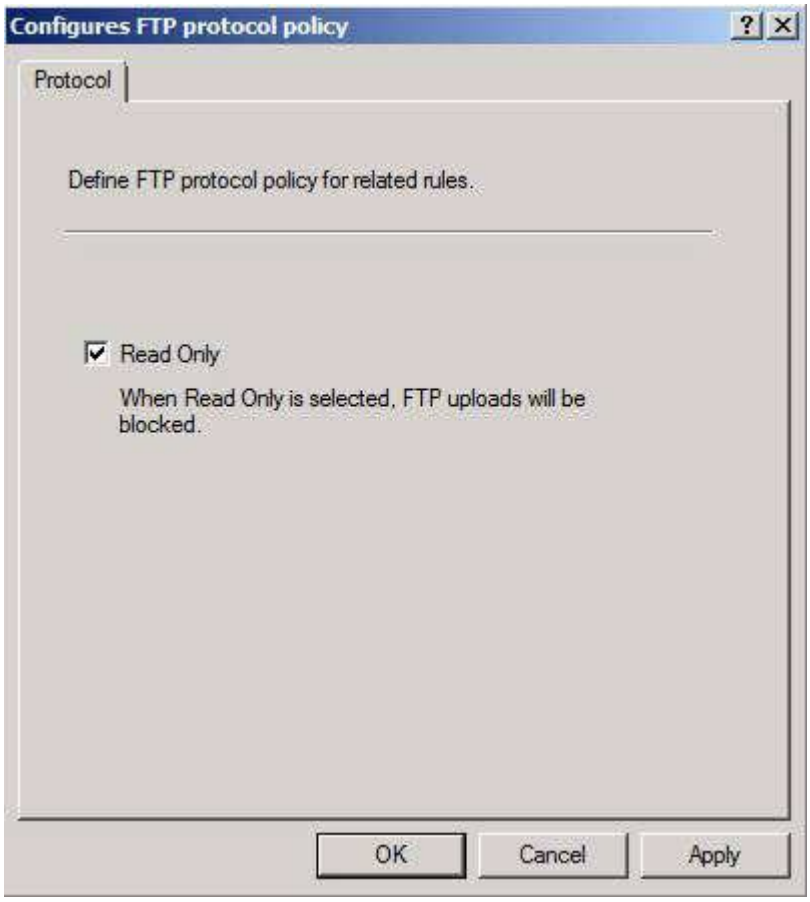

**Figure 3:** Allow write access through TMG

# FTP Server publishing

If you want to allow incoming FTP connections to your internal FTP servers, or to FTP servers located in the DMZ, you have to create server publishing rules if the network relationship between the external and the internal/DMZ network is NAT. If you are using a route network relationship, it is possible to use Firewall rules to allow FTP access.

To gain access to an FTP server in your internal network, create an FTP server publishing rule.

Simply start the new Server Publishing Rule Wizard and follow the instructions.

As the protocol you have to select the FTP Server protocol definition which allows inbound FTP access.

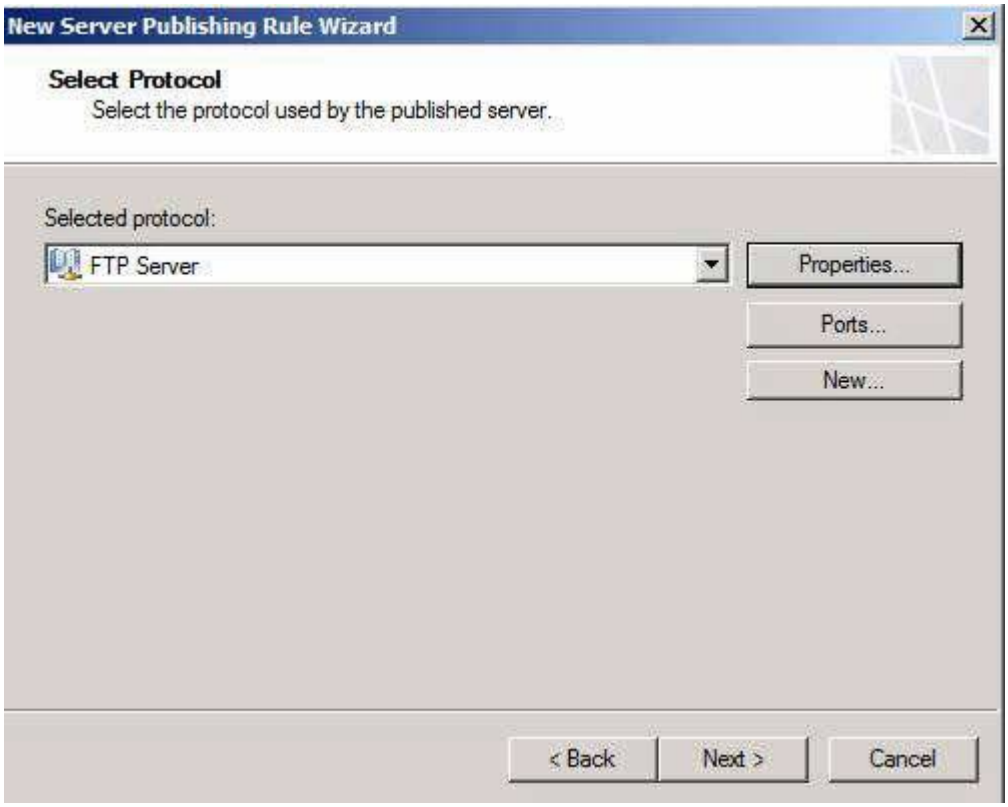


**Figure 4:** Publish the FTP-Server protocol

The standard FTP Server protocol definiton uses the associated standard protocol which can be used for inspection by NIS, if a NIS signature is available.

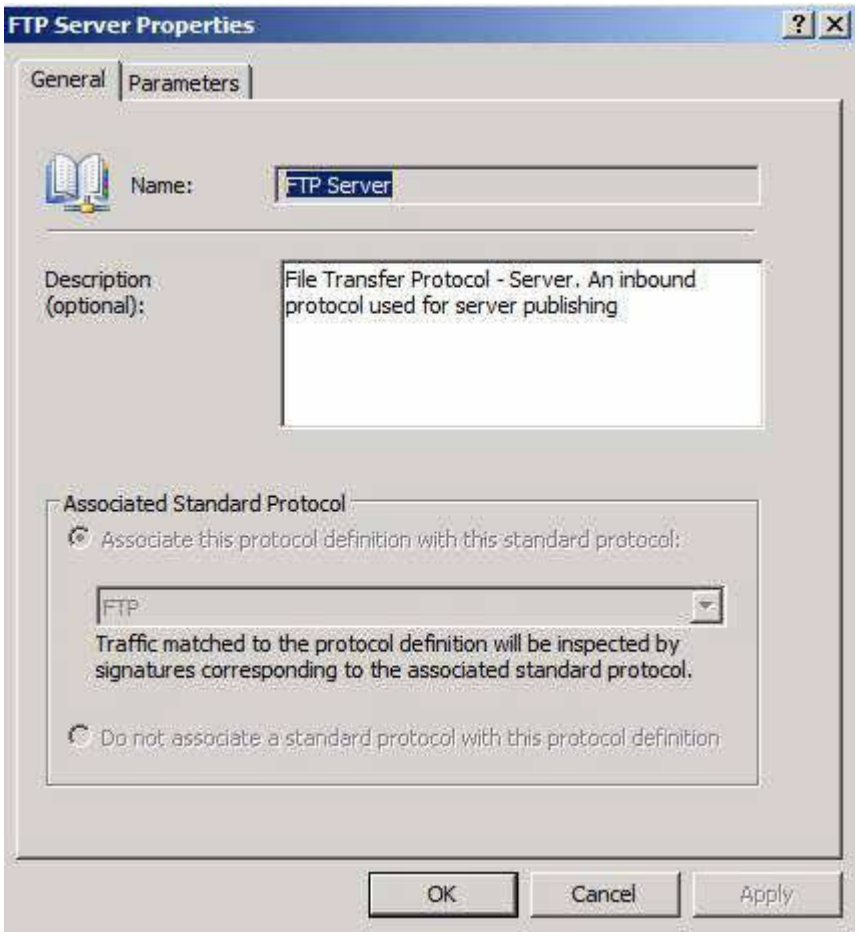


**Figure 5:** FTP-Server protocol properties

The Standard FTP Server protocol definition allows FTP Port 21 TCP for inbound access and the protocol definition is bound to the FTP access filter which is responsible for the FTP protocol port handling (FTP Data and FTP control port).

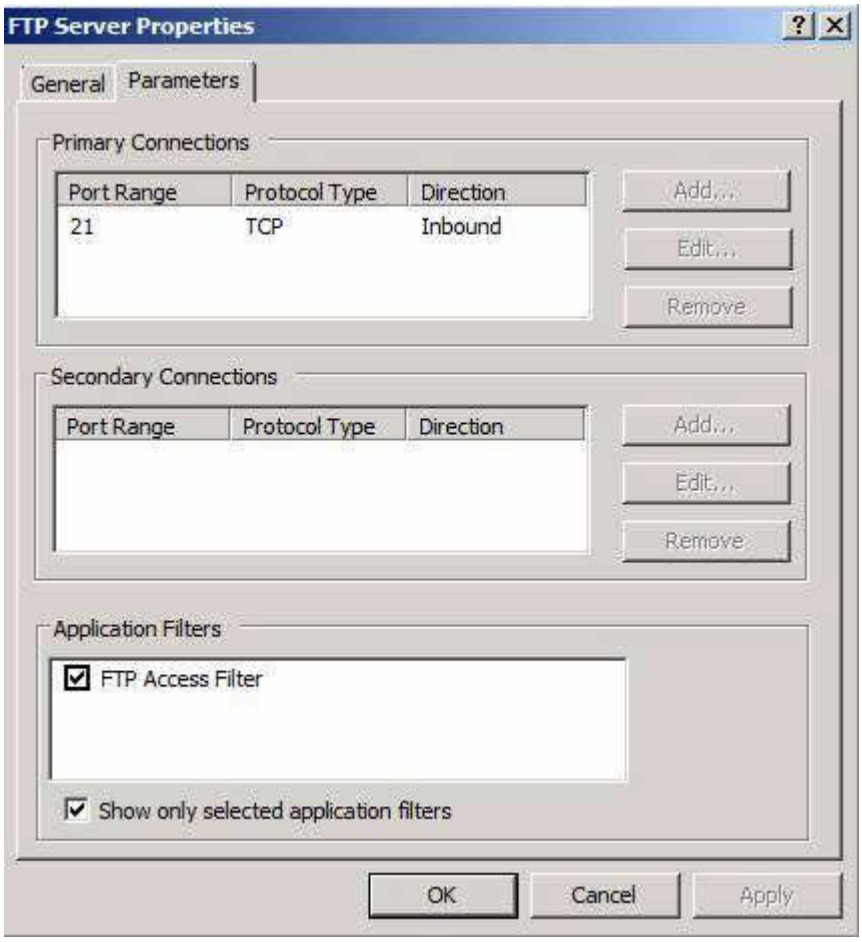


**Figure 6:** FTP ports and FTP Access Filter binding

# Active FTP

One of the changes in Microsoft Forefront TMG is that the Firewall does not allow Active FTP connections by default anymore, for security reasons. You have to manually allow the use of Active FTP connections. It is possible to enable this feature in the properties of the FTP access filter. Navigate to the system node in the TMG management console, select the Applicaton Filters tab, select the FTP Access filter and in the task pane click Configure Selected Filter (Figure 7).

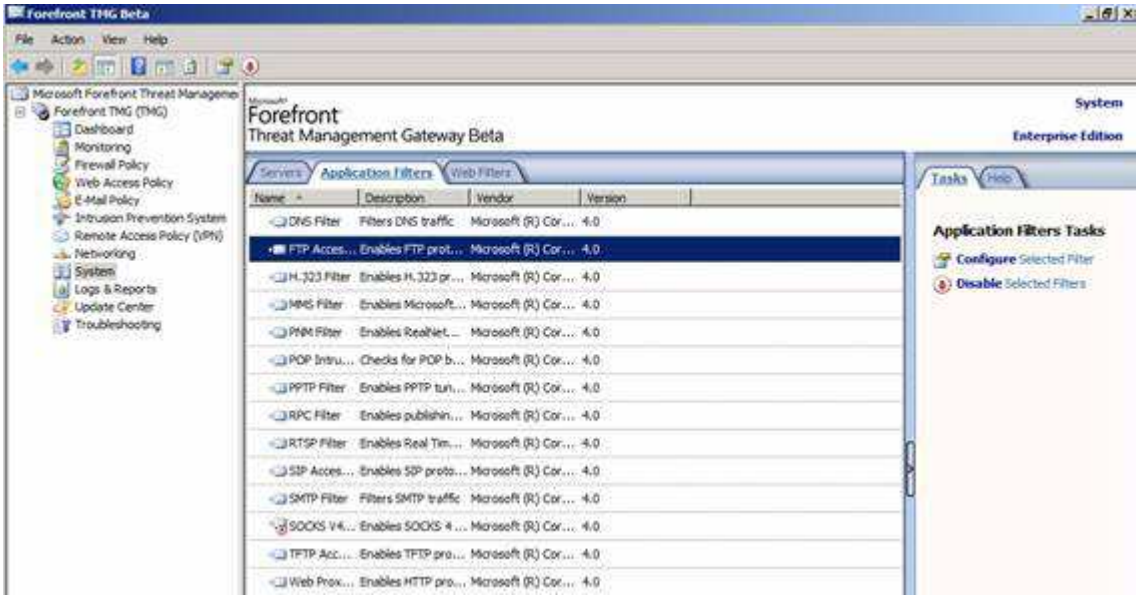


**Figure 7:** FTP Access filter properties

In the FTP access filter properties select the FTP Properties tab and enable the checkbox Allow Active FTP Access and save the configuration to the TMG storage.

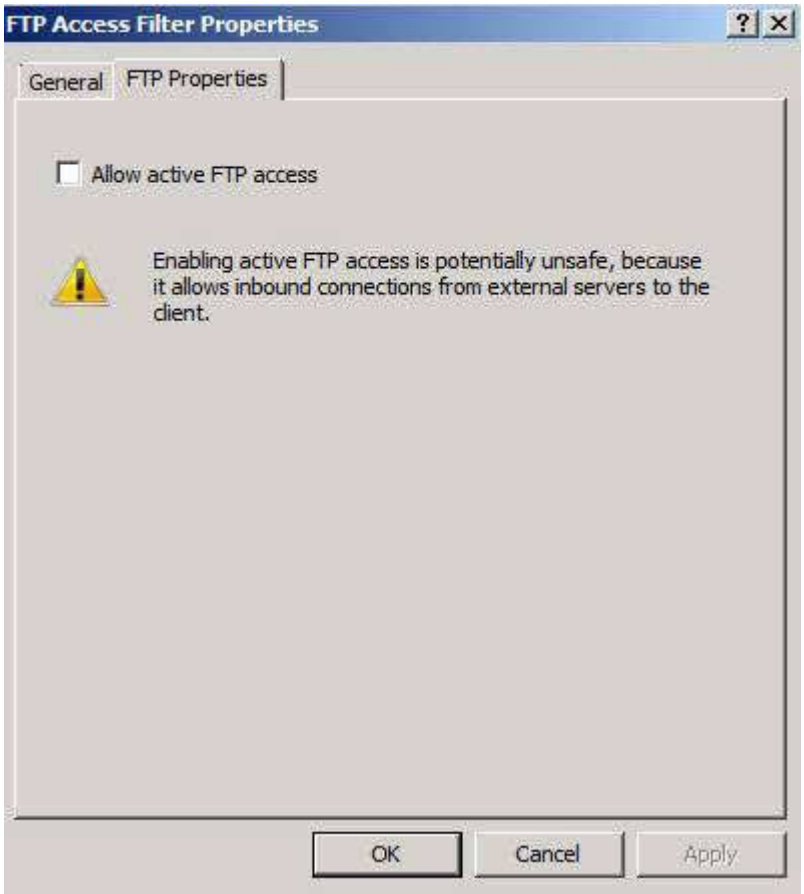


**Figure 8:** Allow Active FTP through TMG

# FTP alerts

Forefront TMG comes with a lot of predefined alert settings for several components and events. One of them is the alert function for the FTP Filter Initialization Warning. This alert informs Administrator when the FTP filter failed to parse the allowed FTP commands.

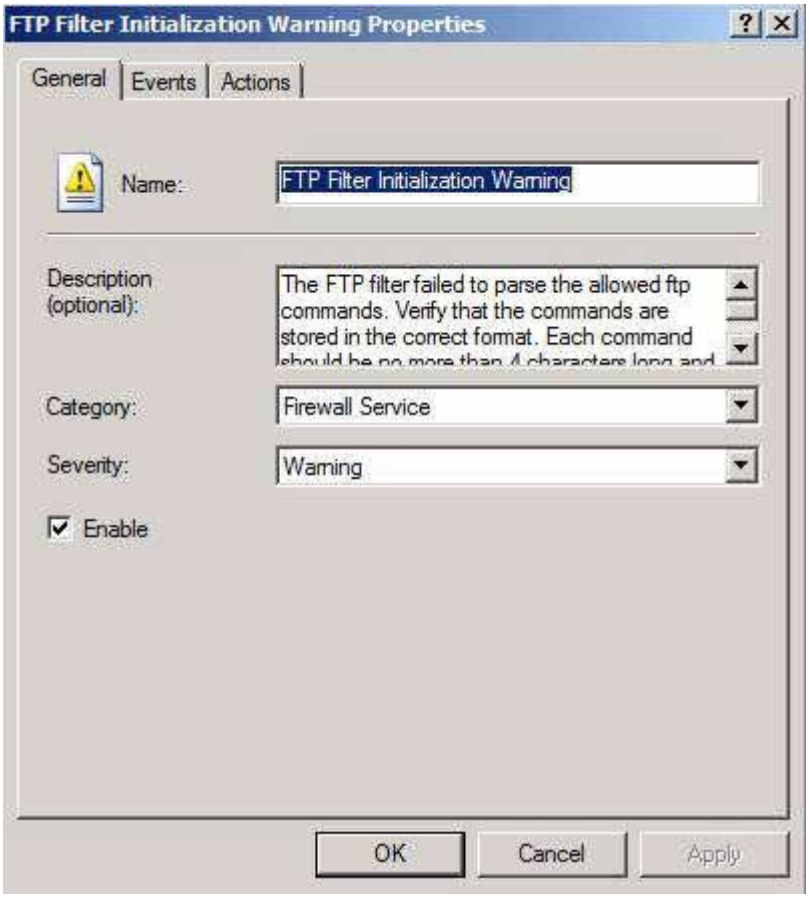


**Figure 9:** Configure FTP alert options

The alert actions are almost the same as in ISA Server 2006, so there are no new things to explain for experienced ISA Administrators.

## Conclusion

In this article, I showed you some ways to allow FTP access through the TMG Server. There are some pitfalls for a successful FTP implementation. One of the pitfalls is that since the introduction of ISA Server 2004, allowing FTP write access through the Firewall and the other pitfall is new to Forefront TMG. Forefront TMG does not allow Active Mode FTP connections by default, so you have to manually activate this feature if you really need this type of special configuration.

# Publishing an FTP server

https://technet.microsoft.com/en-us/library/cc995163.aspx

## To publish an FTP server

1. In the Forefront TMG Management console tree, click **Firewall Policy**.
2. In the task pane, on the **Tasks** tab, click **Publish Non-Web Server Protocols** to open the New Server Publishing Rule Wizard.
3. Complete the New Server Publishing Rule Wizard as outlined in the following table.

| Page | Field or property | Setting or action |
|---|---|---|

| | | |
|---|---|---|
| **Welcome to the New Server Publishing Wizard** | **Server publishing rule name** | Type a name for the protocol definition. For example, type:<br>**Publish FTP Server** |
| **Select Server** | **Server IP address** | Type the IP address of the FTP server that you want to publish. |
| **Select Protocol** | **Selected protocol** | From the drop-down list, select **FTP Server**. Then click **Ports** if you want to override the default ports in the protocol definition. |
| **Ports** (appears only if you click **Ports** on the **Select Protocol** page) | **Firewall Ports** | Select one of the following:<br>o **Publish using the default port defined in the protocol definition**. With this option, Forefront TMG accepts incoming client requests on port 21.<br>o **Publish on this port instead of the default port**. With this option, Forefront TMG accepts incoming client requests on the nonstandard port specified, and then forwards them to the designated port on the published server. |
| | **Published Server Ports** | Select one of the following:<br>o **Send requests to the default port on the published server**. With this option, Forefront TMG accepts requests for the published service on port 21.<br>o **Send requests to this port on the published server**. With this option, Forefront TMG accepts requests for the published service on a port other than port 21. |
| | **Source Ports** | Select one of the following:<br>o **Allow traffic from any allowed source port**. With this option, Forefront TMG accepts requests from any port on allowed client computers.<br>o **Limit access to traffic from this range of source ports**. With this option, Forefront TMG accepts requests only from the ports that you specify. |
| **Network Listener IP Addresses** | **Listen for requests from these networks** | Select the **External** network. To select specific IP addresses on which Forefront TMG will listen, click **Addresses**, and then select **Specified IP Addresses on the Forefront TMG computer in the selected network**. In the **Available IP Addresses** list, select the appropriate IP address, click **Add**, and then click **OK**. |
| **Completing the New Server Publishing Wizard** | | Review the settings, and then click **Finish**. |

4. If you want to enable FTP uploads, perform the following steps.
    1. In the details pane, right-click the name of the rule that you just created.
    2. Click **Configure FTP**.
    3. On the **Configure FTP protocol policy** page, clear **Read Only**.
    4. Click **OK**.
5. In the details pane, click the **Apply** button to save and update the configuration, and then click **OK**.

**Notes**

- For more information about server publishing, see Server Publishing Concepts.
- When you create an FTP server publishing rule, the FTP Access Filter is initially configured to block FTP uploads.
- By default, client requests that are forwarded by Forefront TMG to the published server appear to come from the IP address of the original client. In this case, the default gateway on the FTP server must be set to the IP address of the network adapter on the Forefront TMG computer through which the FTP server connects to it. As an alternative, you can configure your server publishing rule so that forwarded client requests will appear to come from the Forefront TMG computer on the **To** tab of the server publishing rule's properties.
- Server publishing rules are typically used when there is a network address translation (NAT) relationship defined by a network rule between the network on which the clients sending requests to the published server are located and the network on which the published server is located. Server publishing rules can also be used when the network rule between the client network and the network where the server is located defines a routing relationship. However, in this case, the clients must send requests directly to the IP address of the published server.
- If you are publishing an FTP server on the Forefront TMG computer, the published server IP address can be either the IP address of the network adapter of the Forefront TMG computer in the External network or the IP address of the network adapter of the Forefront TMG computer in the protected network.
- Server publishing rules are not supported in a single network adapter configuration.