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

Microsoft Forefront TMG – FTP and FTP Server publishing

Abstract

In this article, I will give you show you the ways how you could 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

First, keep in mind that the information in this article are based on a release candidate version of Microsoft Forefront TMG and are 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 exiting features.

One of the features of Forefront TMG is to allow FTP server traffic through the Firewall in both directions in form of Firewall access rules for outbound FTP access and with server publishing rules for inbound FTP access through a published FTP Server which 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 some high level steps to create a Firewall rule which allows 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 be default, after the FTP access rule has been created, the rule only allows FTP read only access for security purposes 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, click Configure FTP.

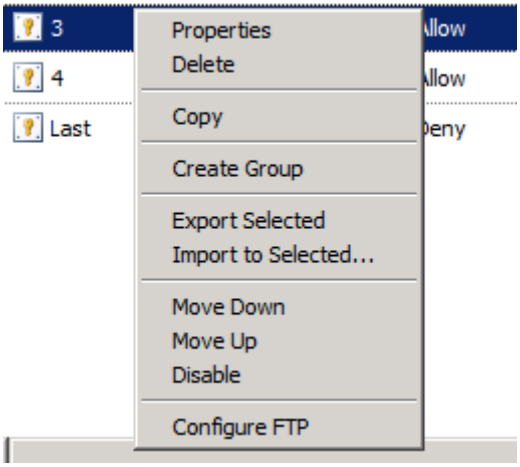

Figure 2: Configure FTP

All you have to do is to remove the read only flag and after a new FTP connection is established users have the permission to do FTP uploads.

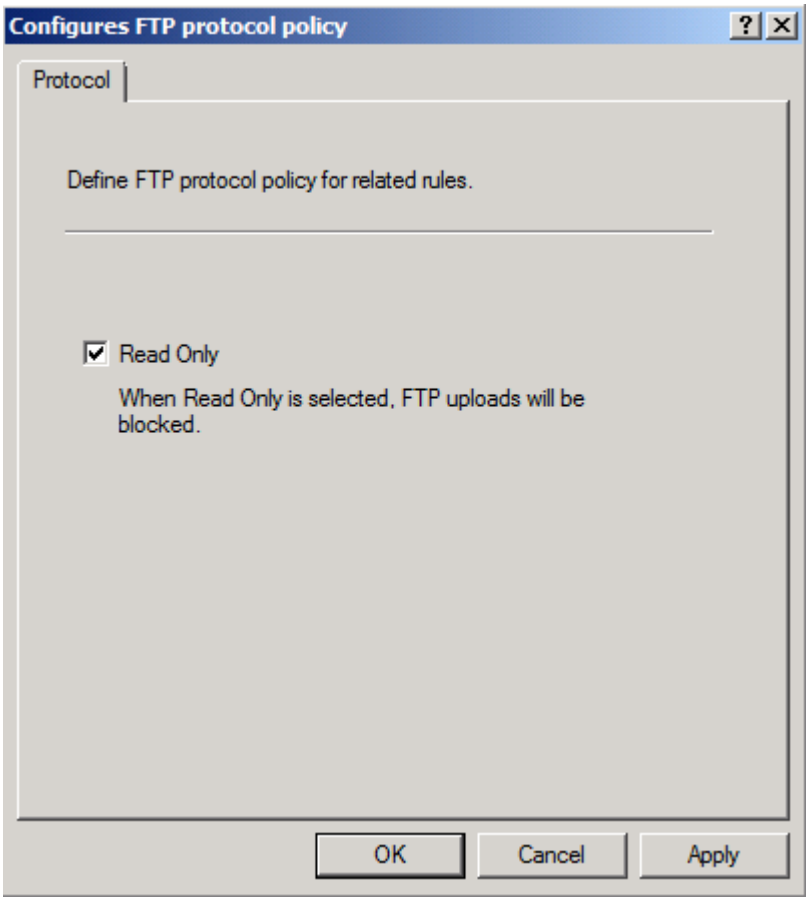

Figure 3: Allow write access through TMG

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 rule 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.

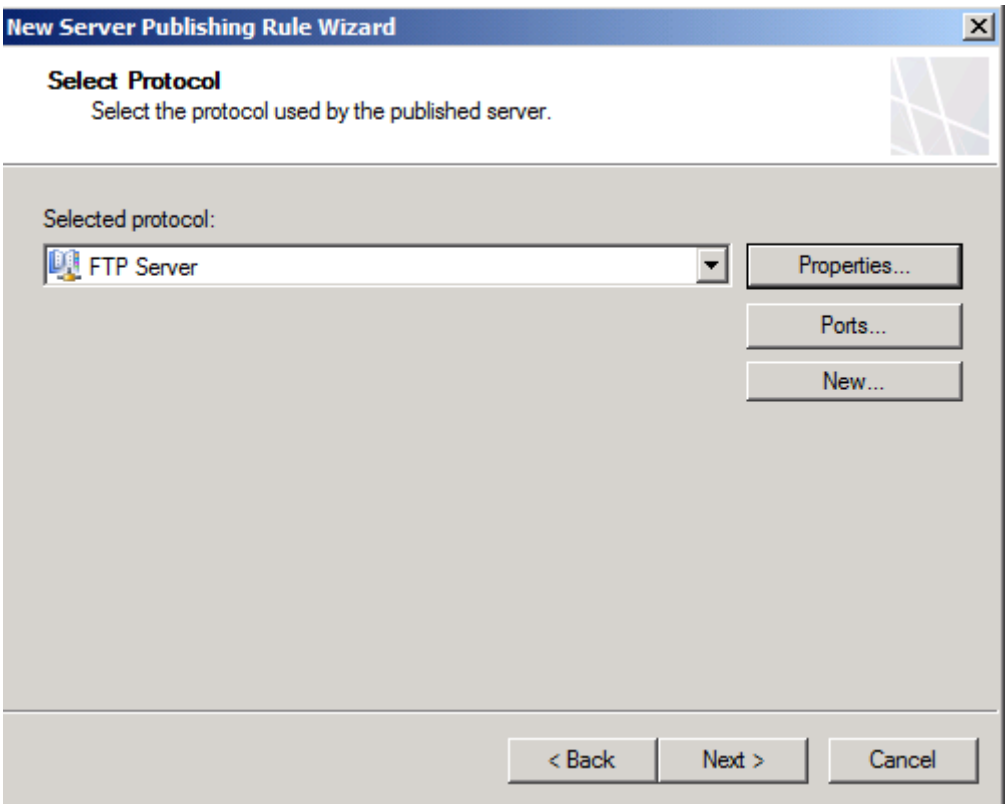

Figure 4: Publish the FTP-Server protocol

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.

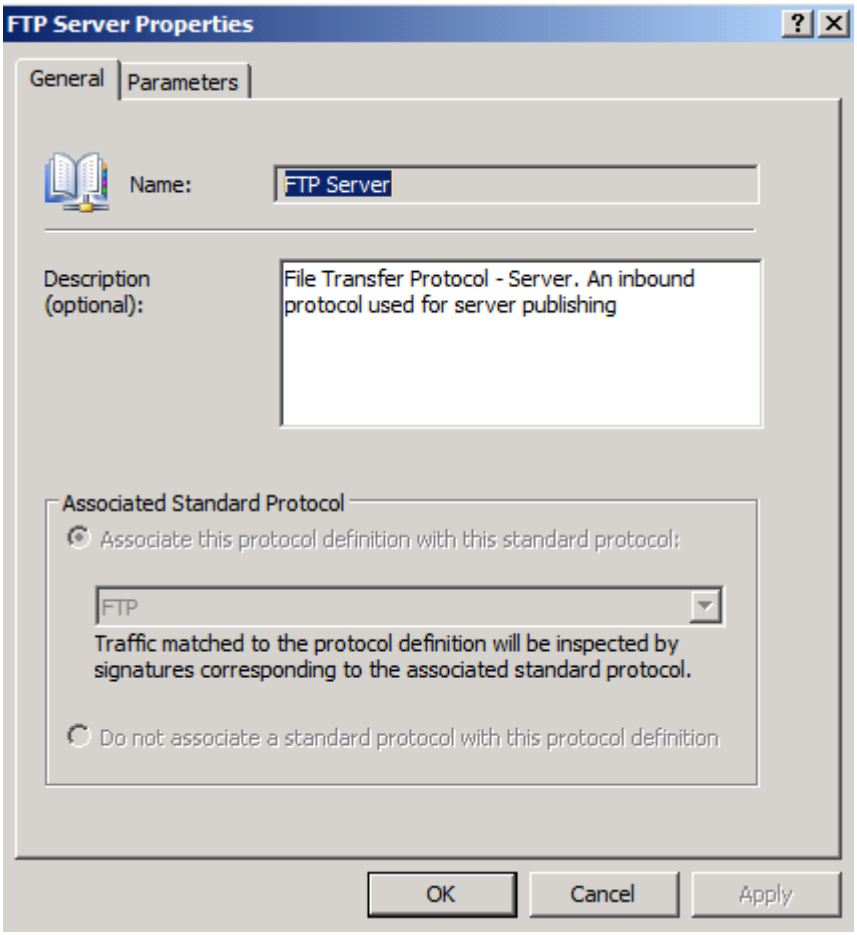

Figure 5: FTP-Server protocol properties

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).

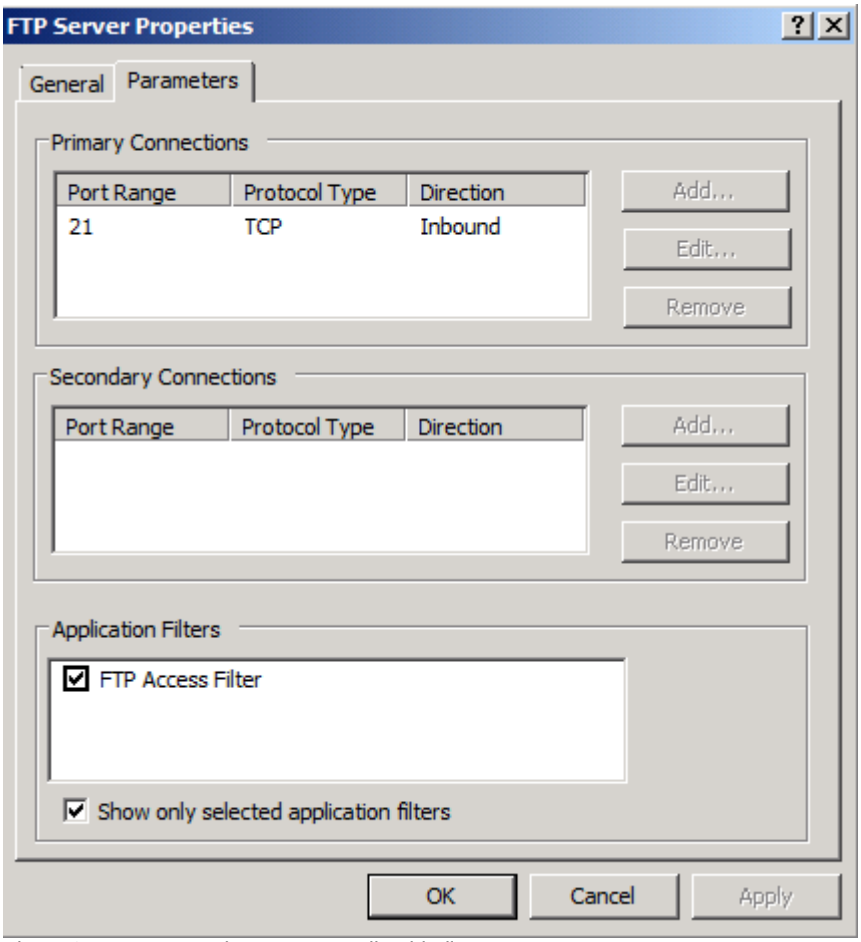

Figure 6: FTP ports and FTP Access Filter binding

Active FTP

One of the changes in Microsoft Forefront TMG is that the Firewall no more allows Active FTP connections by default 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, as shown in the following picture.

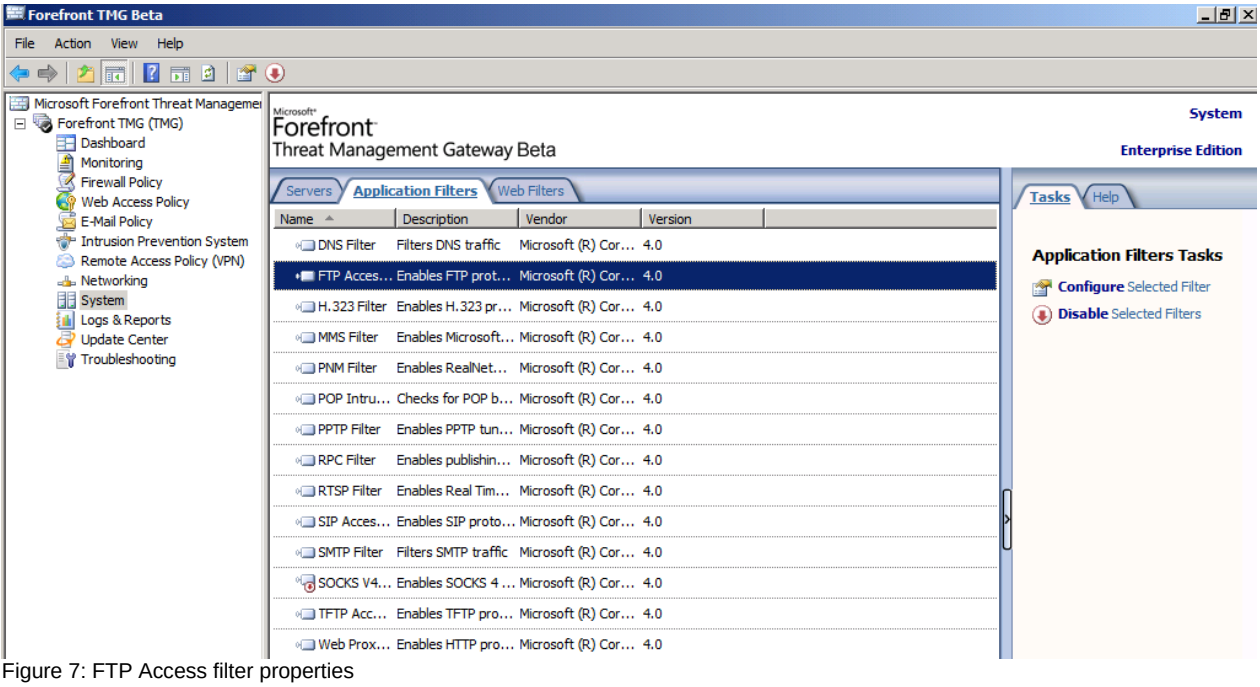

Figure 7: FTP Access filter properties

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.

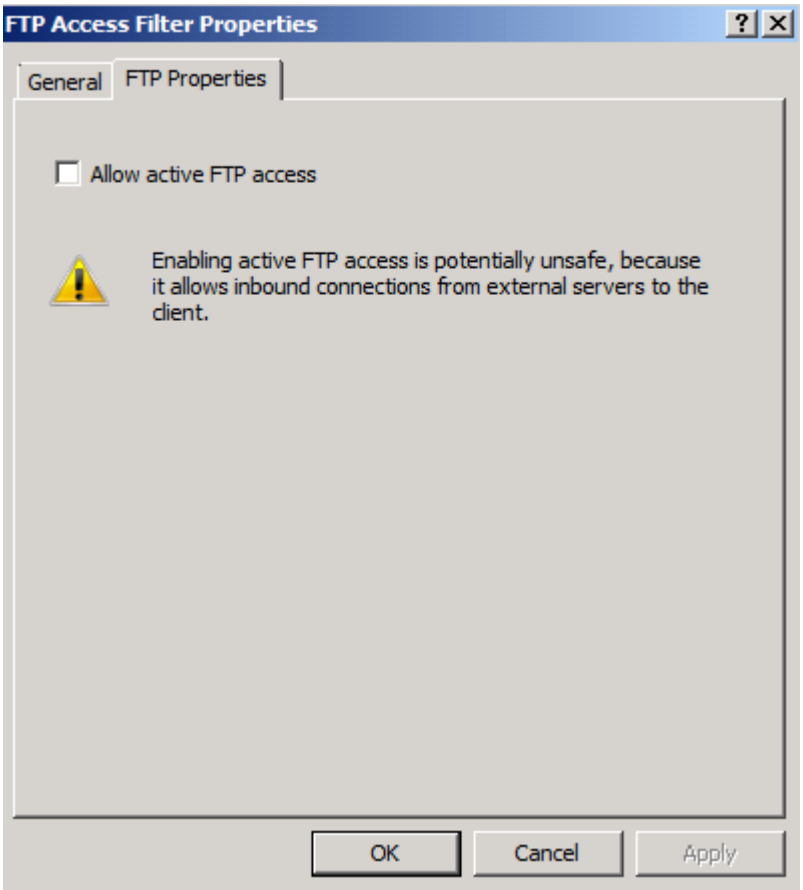

Figure 8: Allow Active FTP through TMG

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.

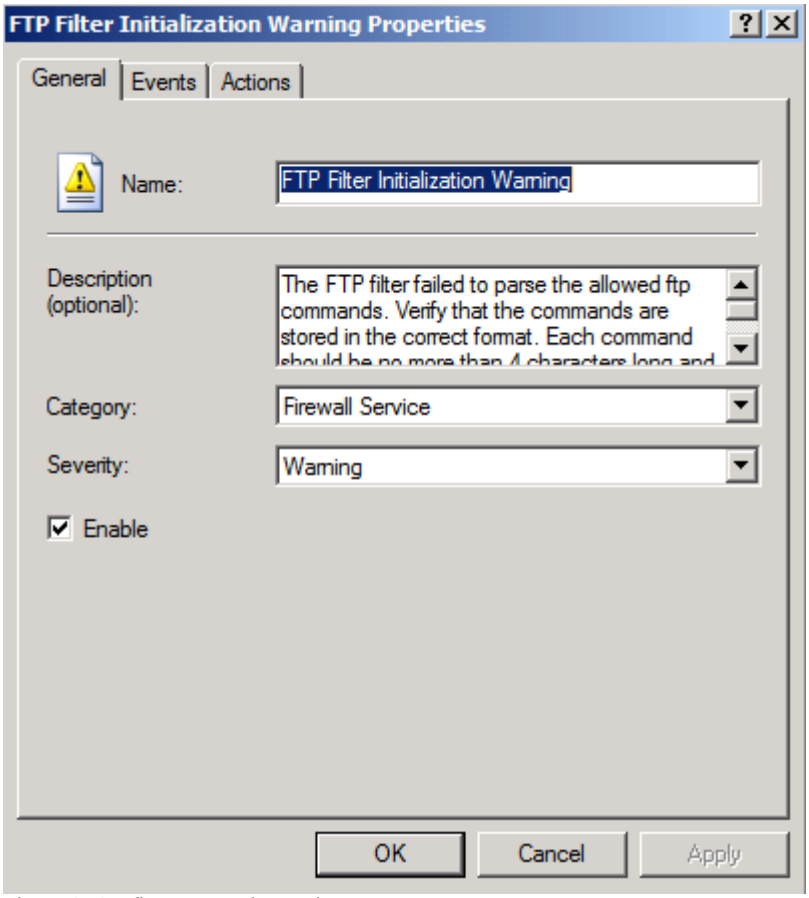

Figure 9: Configure FTP alert options

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 known since ISA Server 2004 how to allow FTP write access through the Firewall and the other pitfall is new to Forefront TMG. Forefront TMG doesn't allow Active Mode FTP connections by default, so you have to manually activate this feature if you really need this type of special configuration.

Related links

Publishing an FTP Server
http://technet.microsoft.com/en-us/library/cc995163.aspx