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

Microsoft Forefront TMG – Best Practice Firewall policy rules

Abstract

In this article we will talk about best practices when implementing Firewall policy rules for outgoing traffic or for incoming traffic with Server- and Webserver publishing rules.

Let's begin

Forefront TMG uses many of configuration elements for creating Firewall policy rules based on several objects.

The first configuration is to create the required networking with Forefront TMG. Basically you must create networks and network relationships from type ROUTE or NAT.

After a Standard Forefront TMG installation there are several predefined network objects. For example there are the following networks:

- Internal – contains all IP addresses of the Internal IP address ranges
- External – represents the “Internet” – the untrusted network and contains all IP addresses which are not part of other TMG networks
- VPN-Clients – A dynamic network object which contains all clients which connects via VPN to the TMG Server
- LocalHost – The TMG Server itself with all connected network adapters.

The network objects must be linked with a network relationship from type ROUTE or NAT depending on your internal IP address environment. Typically you will use NAT when you wants to allow clients with private IP addresses access to the Internet and ROUTE when you have a DMZ for example where webservers are located with public IP addresses.

After a Standard Forefront TMG installation there are several network rules created by Forefront TMG. For example:

- A ROUTE relationship from LocalHost to the Internal network
- A NAT relationship from the Internal network to the External network

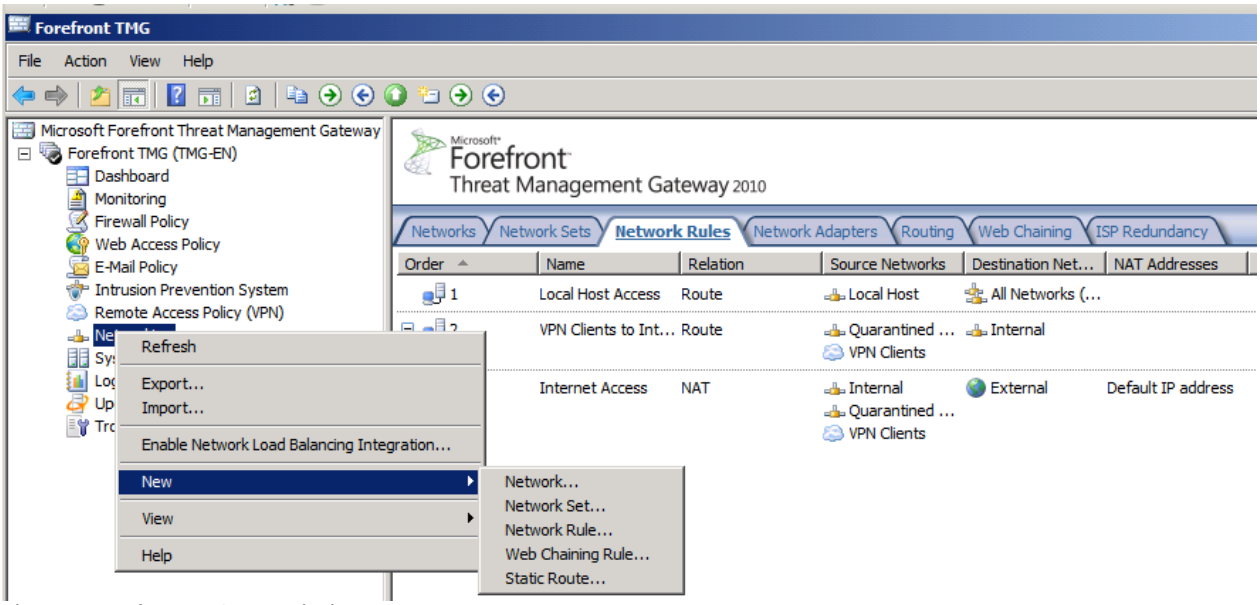

Figure 1: Forefront TMG network elements

After the network objects have been defined and has been associated with network rules it is possible to create Firewall Policy rule to allow or deny access through the TMG Server based on several rule elements with the TMG toolbox.

Firewall Policy rules

After a Standard Forefront TMG installation there are several predefined Firewall Policy rules and Firewall Policy rule elements.
Every Forefront TMG installation comes with three types of Firewall Policies and Firewall Policy rule sets:

- System Policy rule set
- User defined Firewall Policy rule set
- The “Deny all” rule or sometimes called cleanup rule

The System Policy rule set contains a number of predefined Firewall policy rules which exists in every Forefront TMG installation. System Policy rules allows or denies traffic for daily operations from the TMG server to the internal network and to some destinations on the External network. For example:

- Allow Active Directory services access from LocalHost to Internal
- Allow access to Windows update services from Localhost to Microsoft update sites

System Policy rules will be dynamically activated and deactivated by Forefront TMG. For example when you enable Forefront TMG as a VPN Server, the appropriate TMG System policy rules will also be activated.

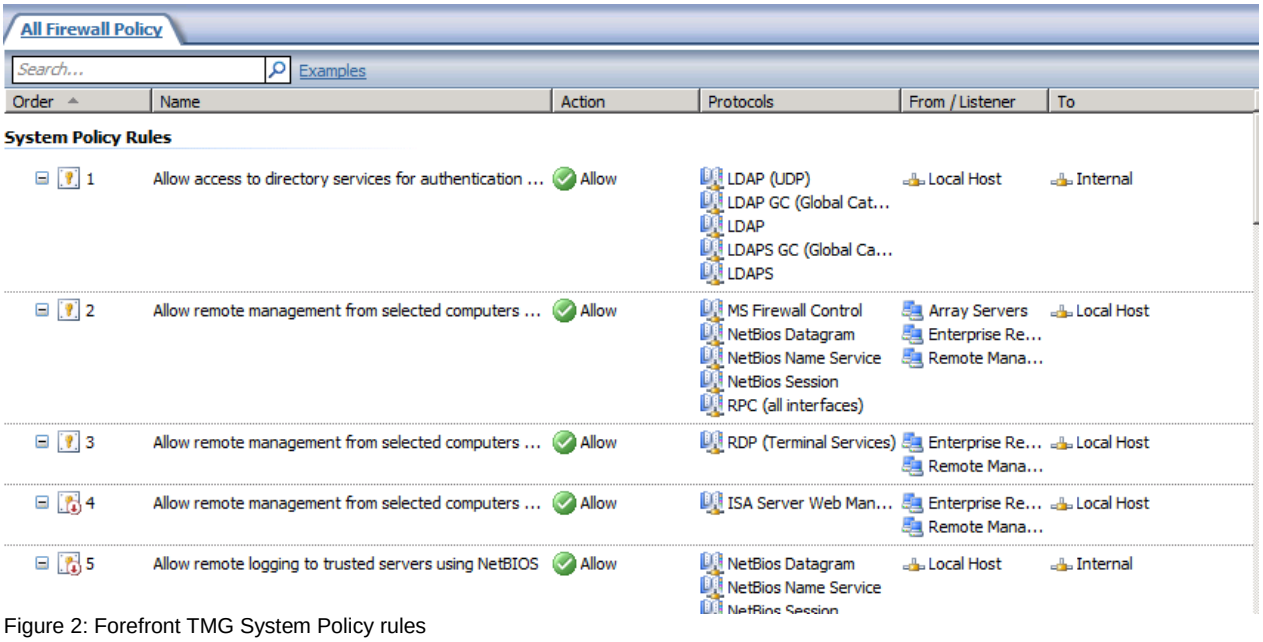

Figure 2: Forefront TMG System Policy rules

The recommended way to configure the System Policy of Forefront TMG is to use the System Policy Editor as shown in the following screenshot.

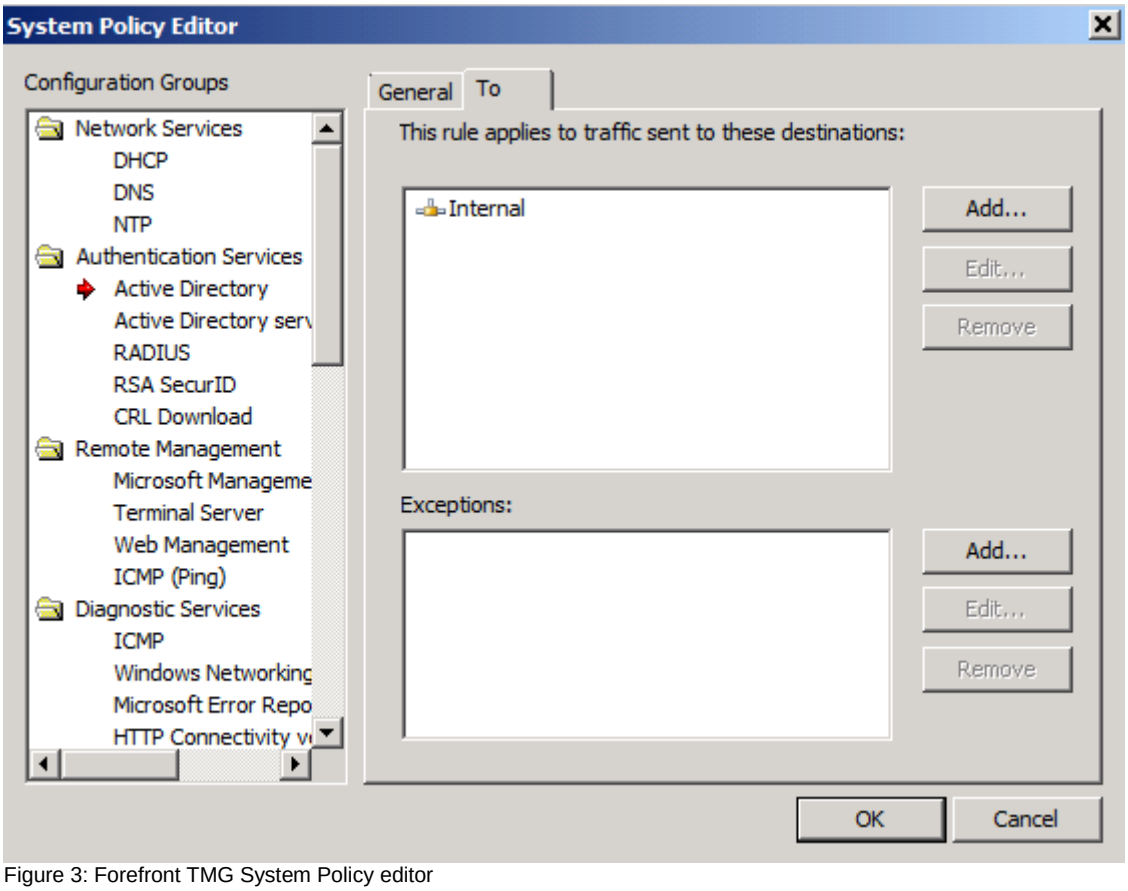

Figure 3: Forefront TMG System Policy editor

User defined Firewall Policy rules

As part of the daily operations Forefront TMG Administrators must create Firewall Policy rules to allow or deny access from internal clients to the Internet and from the Internet to internal resources with the help of Server- and Webserver publishing rules. You can use the Forefront TMG Management console to create the required Firewall policy rules.

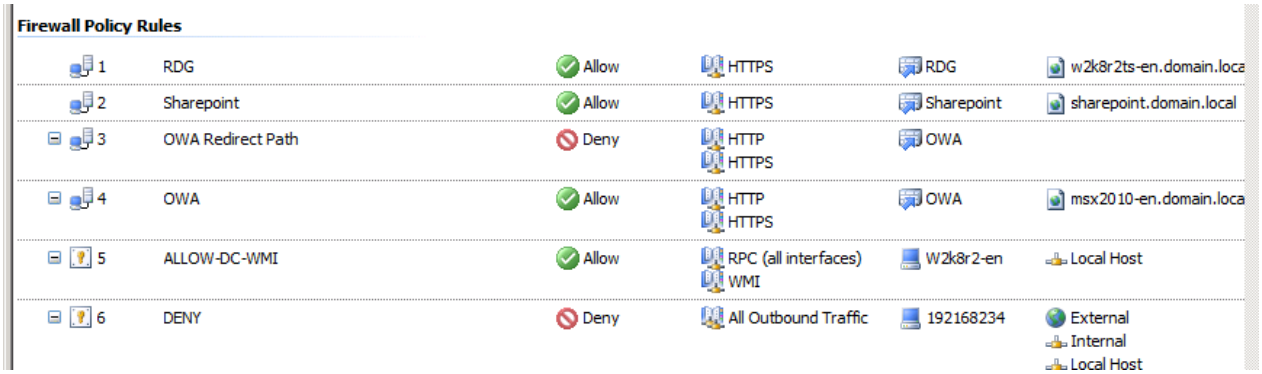

Figure 4: Forefront TMG user defined Firewall Policy rules

Toolbox

All required elements for creating Firewall Policy rules can be found in the Toolbox of the Forefront TMG Management console. The Toolbox consists of several predefined protocol definitions, network objects, computer and URL sets. You are able to create your own protocol definitions to use these protocols in your firewall policy rule.

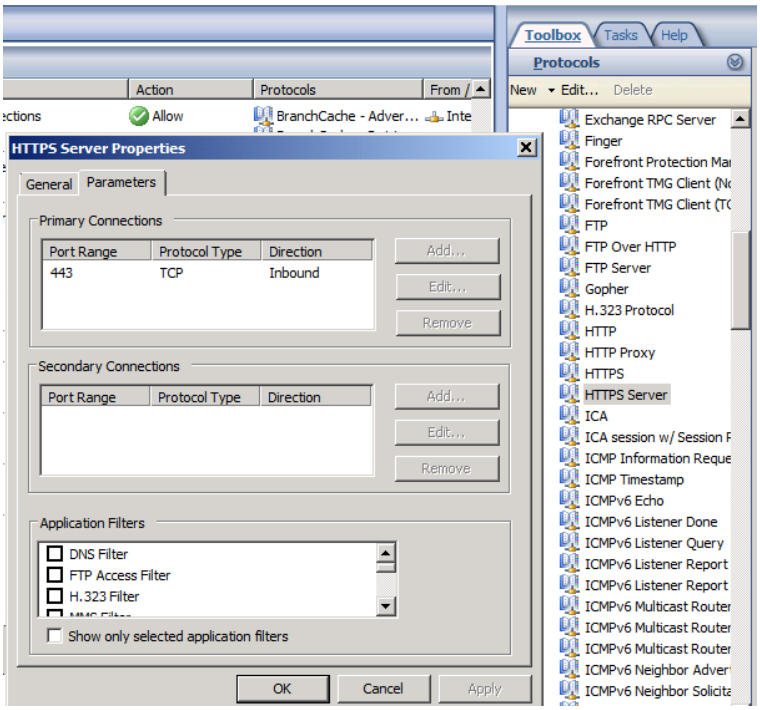

Figure 5: Forefront TMG toolbox and Server protocol properties

Firewall Policy rules best practice

Forefront TMG checks Firewall policy rules in order from top to down with first match.

If the Forefront TMG Standard edition is used, Forefront TMG will evaluate the requests in the following order:

- Network rules
- System Policy rule set
- User defined Firewall Policy rule set
- Deny All (Cleanup rule)

If an allow Firewall policy rule applies to the request, Forefront TMG will allow the request. Specifically, Forefront TMG applies a rule if the request matches the following rule conditions, checking the rule elements in this order:

- Protocol
- From/source address and port
- Schedule
- To/destination addresses, names, URL
- Users
- Content groups

After a matched Firewall policy rule has been found, Forefront TMG stops Firewall policy rule evaluation.
After Firewall Policy rule evaluation has been done Forefront TMG checks the network rules again to determine how the networks are connected. Forefront TMG checks for an existing the Web chaining rules if a Web proxy client tries to open the object.

The evaluation order of Forefront TMG Firewall Policy rules is very important for an efficient Firewall Policy rule set and sometimes also for some performance improvements in daily operations.

General Firewall Policy rule order guidelines

The performance of Forefront TMG may be related to the type of information it requires to evaluate the rules. Because Firewall policy rules are evaluated in order, it may be helpful to place the often used Firewall policy rules near the top of the Firewall Policy rule set, if this order doesn’t conflict for example with Firewall Policy rules which denies access to some destinations.

Simple Firewall Policy rule elements

Some objects of the Forefront TMG toolbox are easy to evaluate without an additional overhead to do some authentication against your internal Active Directory for example:

- Protocol definitions
- Schedules
- All network elements like Computers, Computer sets, IP Subnets and more

Microsoft recommends that you should place Firewall Policy rules with these elements at the top of the Firewall Policy rule set.

Complex Rule Elements

The following Firewall Policy rule elements require additional networking information like DNS name resolution, Active Directory (LDAP, GC) lookup and should be placed at the bottom of the Firewall Policy rule set:

- Domain name sets
- URL sets
- Users
- Content type

Firewall Policy rules which use Application filters

Forefront TMG a Secure Web Access Gateway comes with a lot of additional Application and Web filters which allow the filtering of different protocols. Some examples of those filters are:

- SMTP filter
- HTTP filter
- Malware inspection filter
- Outgoing HTTPS inspection
- FTP Access filter
- GAPA (NIS) filter

Firewall Policy rules which uses these filters will be typically processed slower than Firewall Policy rules without “intelligent” application filter.

General rule order recommendations

Based on this information Microsoft recommends organizing Firewall Policy rules in the following order:

- Global deny rules
- Global allow rules
- Rules for specific computers
- Rules for specific users
- Other allow rules

Global deny rules.

A Global deny rule should be used when you want to deny all users access to specific protocols for example you would like to deny access the use of the SIP protocol from Internal to External for all users.

Global allow rules

A global allow rule for example to allow all users to access FTP servers on the Internet.

Rules for specific computers

Rules that allow or deny access for specific computers, For example you only want to allow you Administration PC to access one Server in the Internet with the RDP protocol.

Rules for specific users, URLs, and MIME types

Firewall policy rules for specific users, or for specific URL or MIME types and with advanced filtering like Malware Inspection, HTTP filtering, Network Inspection System (NIS).

Other allow rules.

At least you should place other allow Firewall policy rule at the end of the Firewall Policy rule set when they doesn't match the other criteria's for placing Firewall policy rules.

Attention*:*

Webserver- and Server publishing rules can be placed anywhere in the Firewall Policy rule set but I recommend grouping these publishing rules to have a better overview about the Firewall policy rules.

Conclusion

In this article we started with a short overview about Forefront TMG networks, network rule and Firewall policy rule elements and rule to give you an overview about these essential daily administration tasks. After that I tried to show you some guidelines for best practices how to create an efficient Firewall policy with Forefront TMG and how important the order of Firewall Policy rule may be.

Related links

ISA Firewall Best Practices, Tips and Tricks (Part 1) ISA Firewall Best Practices, Tips and Tricks (Part 1)
http://www.isaserver.org/tutorials/2004bestpractices-p1.html
FW_FWIntro
http://technet.microsoft.com/en-us/library/bb838971.aspx
Best Practices Firewall Policy for ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794766.aspx
System Policy rules
http://technet.microsoft.com/de-de/library/cc441740.aspx