Configure Web Proxy Chaining in Forefront TMG 2010 - Part 1

In this series, I will show you a typical deployment scenario and how to configure web proxy chaining in Forefront Threat Management Gateway (TMG) 2010.

In this series we will show you a typical deployment scenario and how to configure web proxy chaining in Forefront Threat Management Gateway (TMG) 2010 .

Web proxy chaining is an effective way to distribute web proxy traffic in an organization, contributing to reducing bandwidth consumption on low-speed WAN links, reducing resource usage on proxy servers in documents. main room, or delegated administration to remote site administrators. Web proxy chaining is a configuration in which a proxy server (called a *downstream* proxy server) is configured to forward requests to another proxy server (called *upstream* proxy server) instead of retrieving the contents. directly from the Internet. Downstream proxy server may or may not have a direct connection to the Internet. In the first part of this two-part series, let's take a look at a deployment scenario and we will show you how to configure web proxy chaining in Forefront Threat Management Gateway (TMG) 2010. .

Web Proxy Chaining

Before proceeding, an important issue to be clarified is that the web proxy chaining only applies to traffic handled by the web proxy filter; means traffic generated by web proxy client clients. Web proxy chaining has no effect on TMG Firewall Client or SecureNET traffic. To take advantage of web proxy chaining features available in TMG, we need to configure clients to use proxy servers, either by entering a proxy server manually or by using one of the automatic configuration options (DNS or DHCP), using group policy, or by deploying TMG Firewall Client with the appropriate proxy server settings.

Configuration

A common web proxy chaining deployment scenario is when a proxy server (or array) is located in the main office, another proxy server (or array) is located at the remote branch office (see in the map below). Users at the main office are configured to use the main proxy server for Internet access. Users at the branch office are configured to use their local proxy server, which is the proxy server configured to forward requests to the upstream proxy server located at the main office.

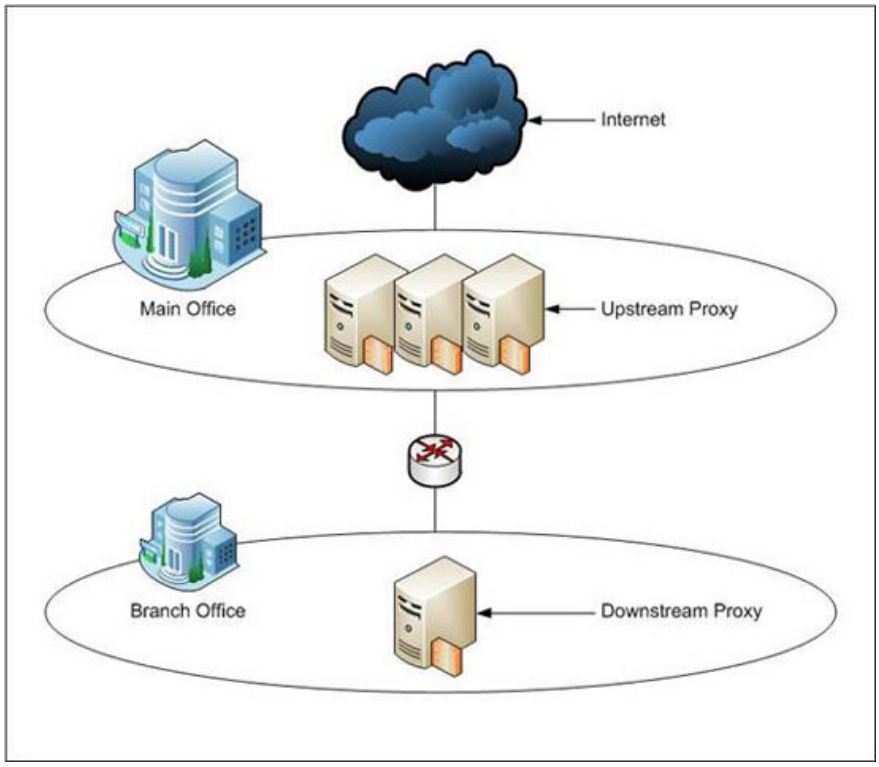

Figure 1

Web proxy chaining is enabled by creating *web chaining rules* . These rules determine how the firewall routes the web proxy requests when allowing them. To configure web proxy chaining in this basic scenario, open the TMG management console on the **downstream** proxy server and click the **Networking** button in the console tree.

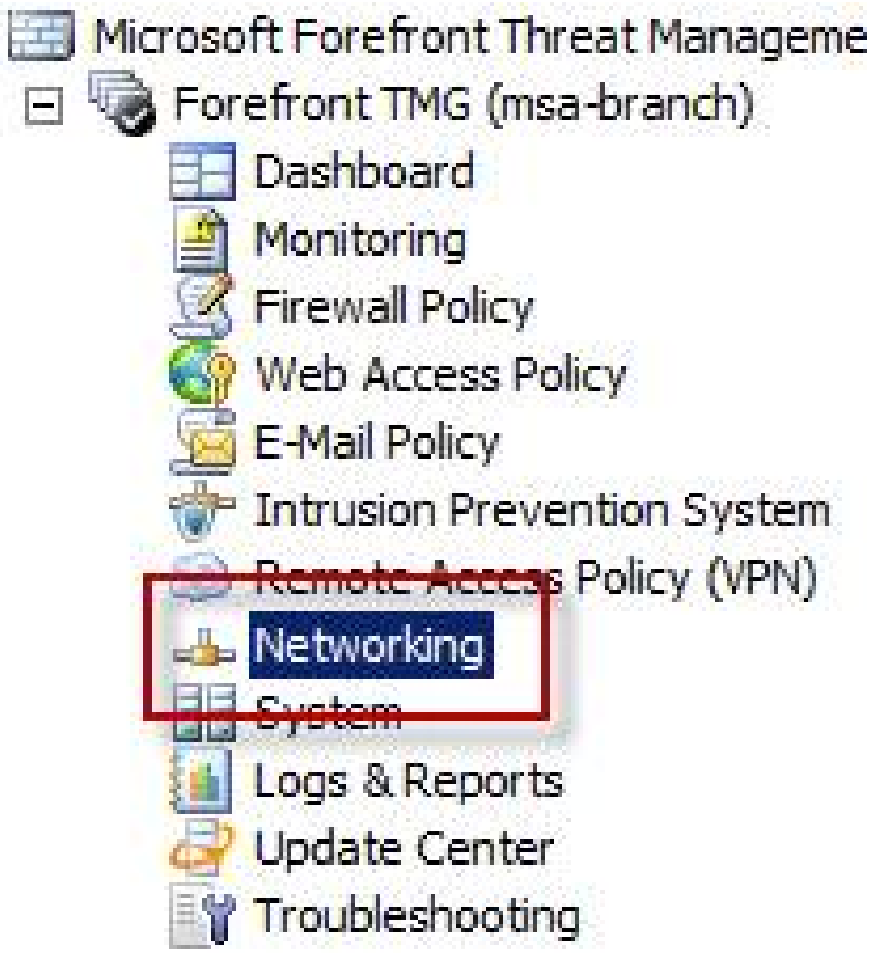

Figure 2

Figure 2: In the main window, select the **Web Chaining** tab, and then in the **Tasks** panel select **Create New Web Chaining Rule** .

Figure 3

When the **New Web Chaining Rule Wizard** opens, name the new web chaining rule.

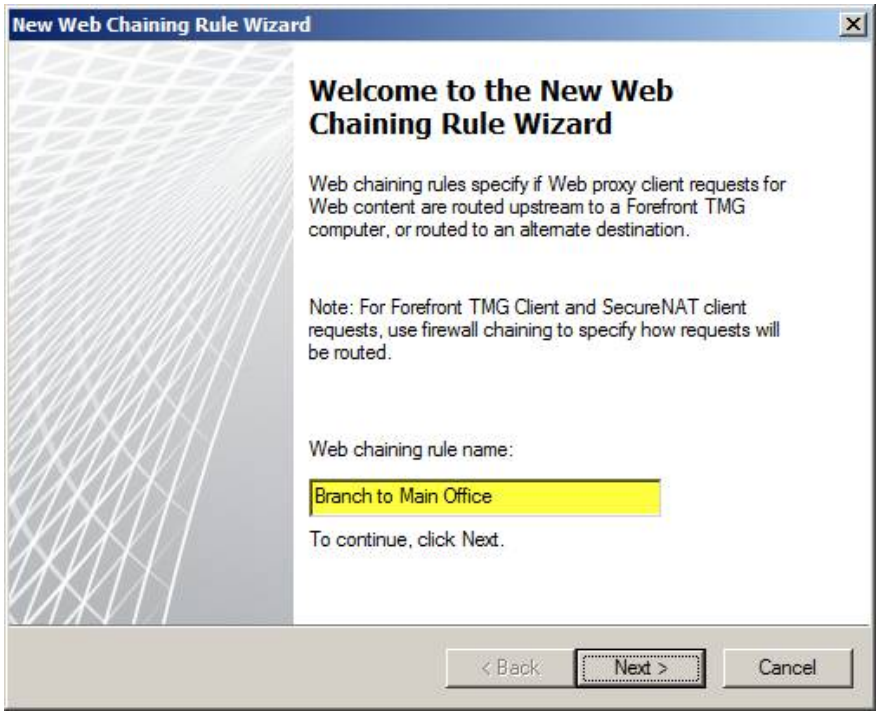

Figure 4

Select the appropriate **Web Chaining Rule Destination** . We have almost no restrictions on the options here, but for demonstration purposes, we only choose to forward all requests to the Internet by selecting the **External** network **.**

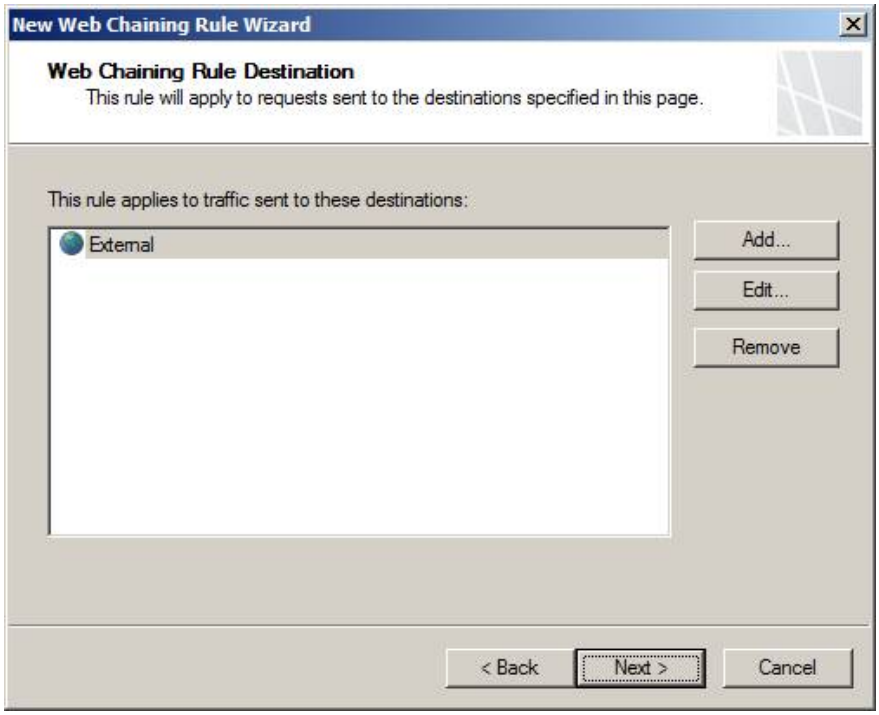

Figure 5

Select the option to transfer the requests to the specified **upstream** server.

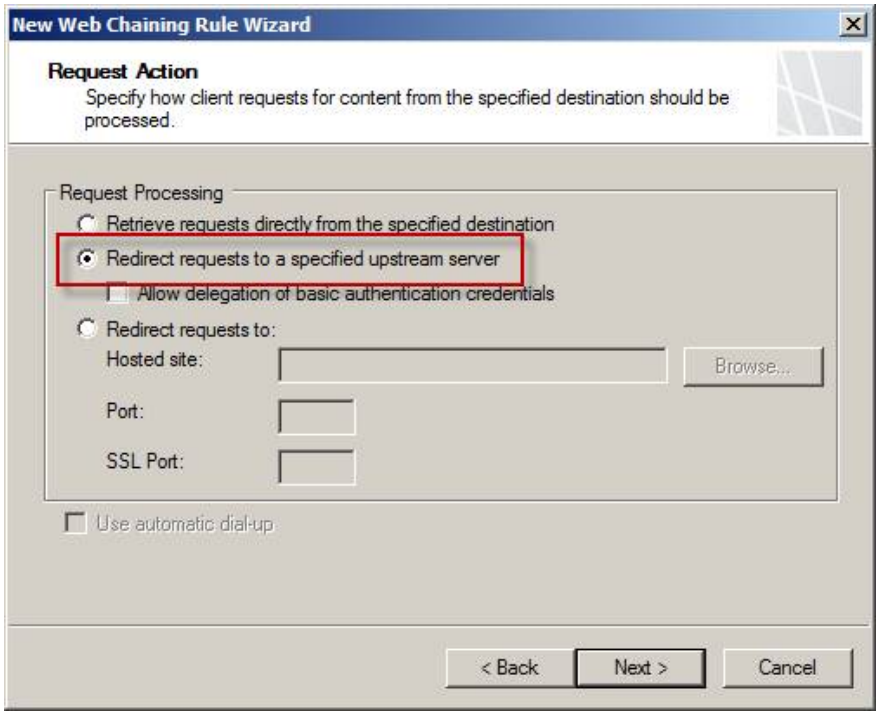

Figure 6

Specify the IP address, hostname or FQDN of upstream proxy server. Unless you have changed the web proxy listening ports on upstream proxy server, you will not need to change the default ports listed here. To **apply the Apply malware check to Web content received from or sent to an upstream proxy** checked only when upstream proxy server does not perform malware inspection, because the malware inspection is not supported on both downstream proxy server and upstream proxy server at the same time. The option to scan for viruses and malware is by you. If you choose to scan on upstream proxy server, you can prevent malicious software from entering the network. If upstream proxy server is aggregating a large number of downstream proxy server requirements, the load will increase significantly and may overload CPU and disk performance, resulting in latency. In this case, scanning downstream servers will help you distribute the load, reducing resource consumption on upstream servers.

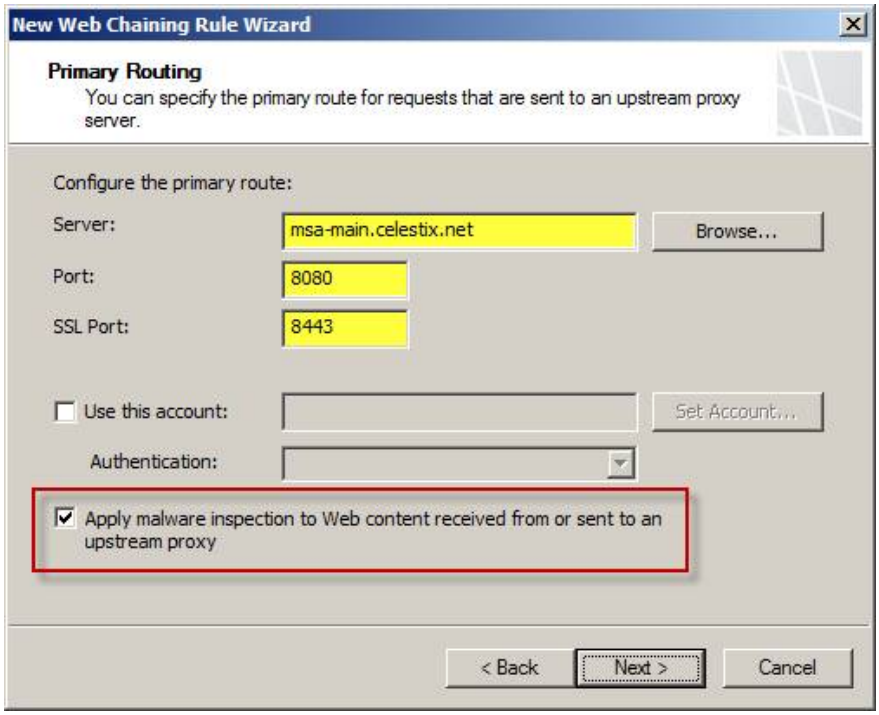

Figure 7

Select the **backup action that is** appropriate for your environment. If the downstream server has a direct connection to the Internet, you can choose the option to **retrieve requests directly from** a destination (**retrieve requests directly from the specified destination**). If there is a proxy server (or array) in another location that can be used as an upstream server, then you can choose the option to **route requests to the upstream server** (**route requests to an upstream server**). (there will be additional information reminders). If the downstream server does not have alternate routes (or is not allowed for corporate security policies), select the default option to **ignore requests** .

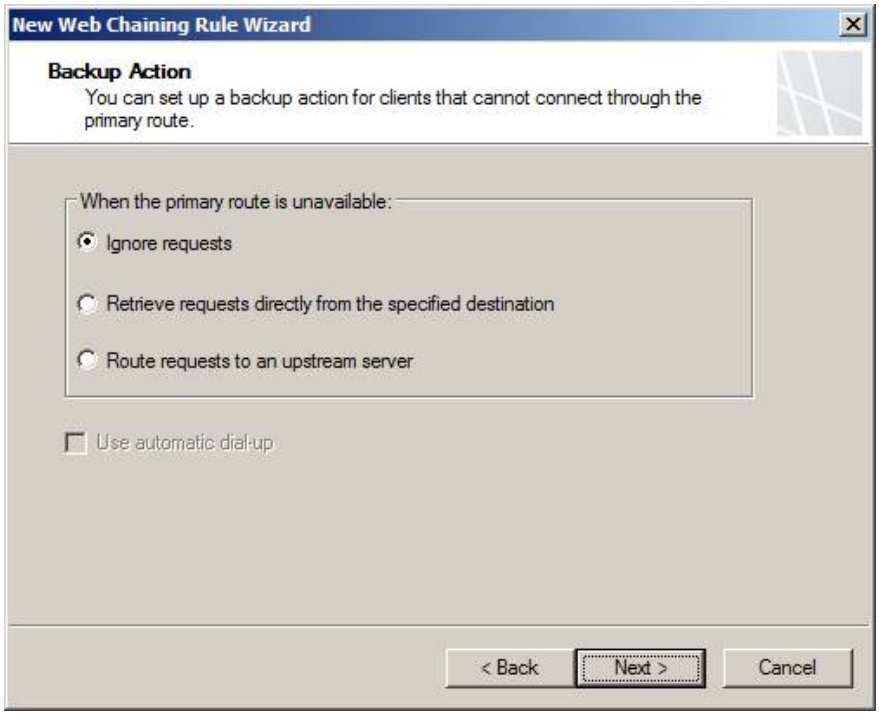

Figure 8

The new rule will now appear in the list. Web chaining rules will be processed in order, so our new rule is preceded by the default rule. Although we have created a new rule here, it is possible to change the default rule to provide the same results.

Figure 9

Note: An important issue to keep in mind is that access rules must be properly placed on the downstream server and upstream to facilitate web access.

Connection restrictions

In many cases, enabling web proxy chaining can cause the server downstream to exceed the connection restrictions enforced by the overflow settings on the upstream server. Upstream servers will receive connection requests from a particular host (downstream server) instead of each individual client. If the server is downstream aggregating requests for a large number of clients, we need to change the default connection restrictions on the upstream server. This can be configured by adding downstream servers to the IP exception list, rather than changing the default restrictions for all hosts. You will find the overflow settings in the TMG management interface by clicking **Intrusion Prevention System** in the interface tree, clicking **Configure Flood Mitigation**

Settings in the main window and then selecting the **IP Exceptions** tab and creating a computer set containing Your downstream servers.

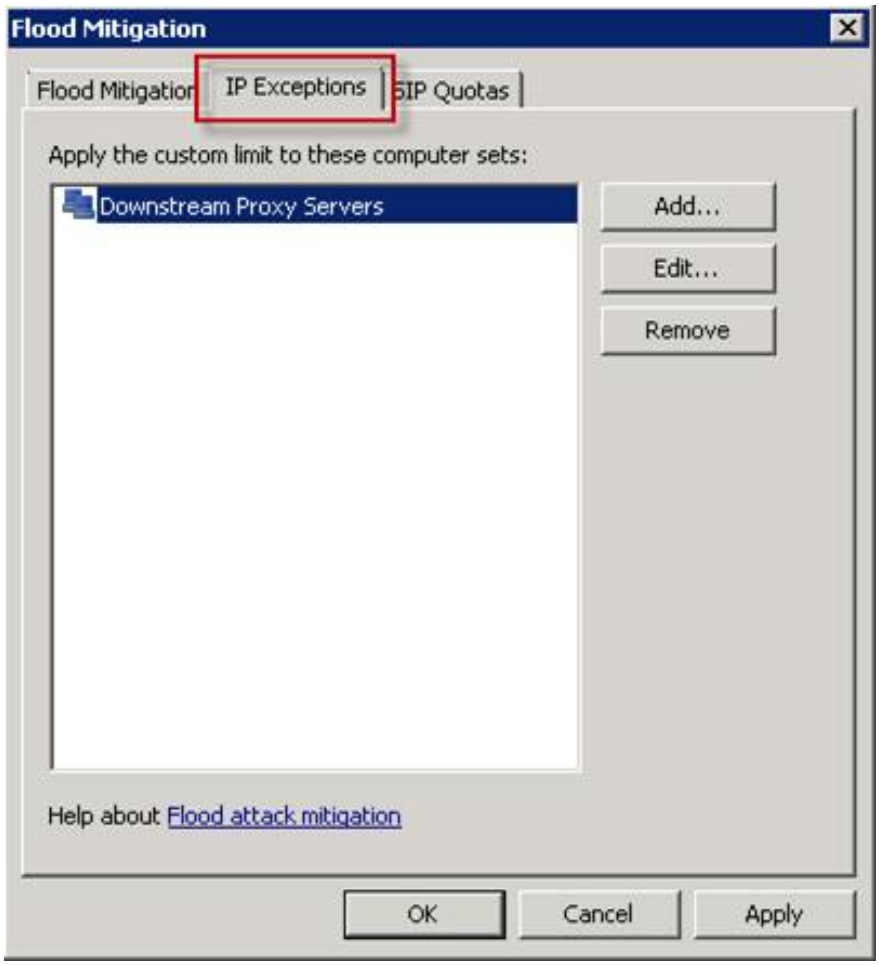

Figure 10

Conclude

Depending on your specific requirements, web proxy chaining configuration may be relatively simple (as discussed here) or can be quite complicated. The example outlined above assumes that all traffic will be routed to the upstream proxy server, and no authentication is required. In many cases, the downstream proxy will have a direct connection to the Internet and only some traffic is routed to the upstream proxy server. Normally an upstream proxy server also requires authentication, so additional plans and configurations are required. In part two of this article series, I will show you some more detailed deployment scenarios.