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

Secure CDP publishing with Forefront TMG and the HTTP-filter

Abstract

In this article we will first cover some basic information about a Public Key infrastructure which uses CRL, OCSP, CDP and AIA information to keep ensure that revoked or not more valid certificates cannot be used to provide secure access to applications. Next I will show you how to securely publish the CDP with Forefront TMG and the help of the HTTP-filter.

Let's begin

A Public Key Infrastructure (PKI) is a combination of certificates, services, policies, software and hardware to manage the complete lifecycle of certificates. This lifecycle includes the creation of certificates, issuing, managing and revoking of certificates. The primary part of a PKI is a Certification Authority which is responsible for issuing and revoking certificates for services, clients, Server, people, Smartcards and many more.

Certification Authorities will be distinguished between private and commercial Certificate Authorities. Each of this CA types has pros and cons. If you are using a private CA, you can use the built in Certificate Authority of the Windows Server 200x Operating System. The following screenshot shows the UI of a Windows Server 2008 R2 Enterprise CA.

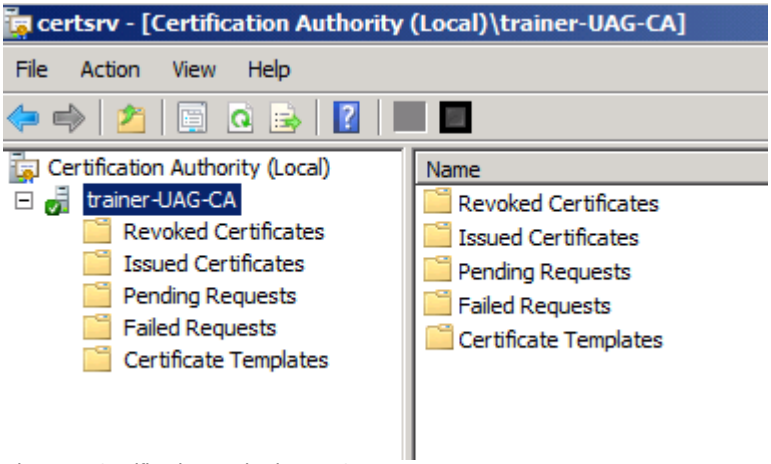

Figure 1: Certification Authority MMC

As mentioned above, a CA is also responsible for revoking certificates, if issued certificates are out of lifetime or if they must be revoked due to certificate compromise, certificate lost and some more reasons.

Depending on the application or service, not all application checks a certificate for revocation but if a revocation check is required the application must know from where it can download the list of revoked certificates.

The path for revoked certificates is defined in the CDP (Certificate Distribution Point). The CDP contains the Certificate Revocation List (CRL) which must be downloaded by the client or application to get informed about the certificate status during a certificate trust check. A Windows Server 2008 R2 CA publishes the CRL to different locations, containing LDAP, Windows file system and HTTP as you can see in the following screenshot.

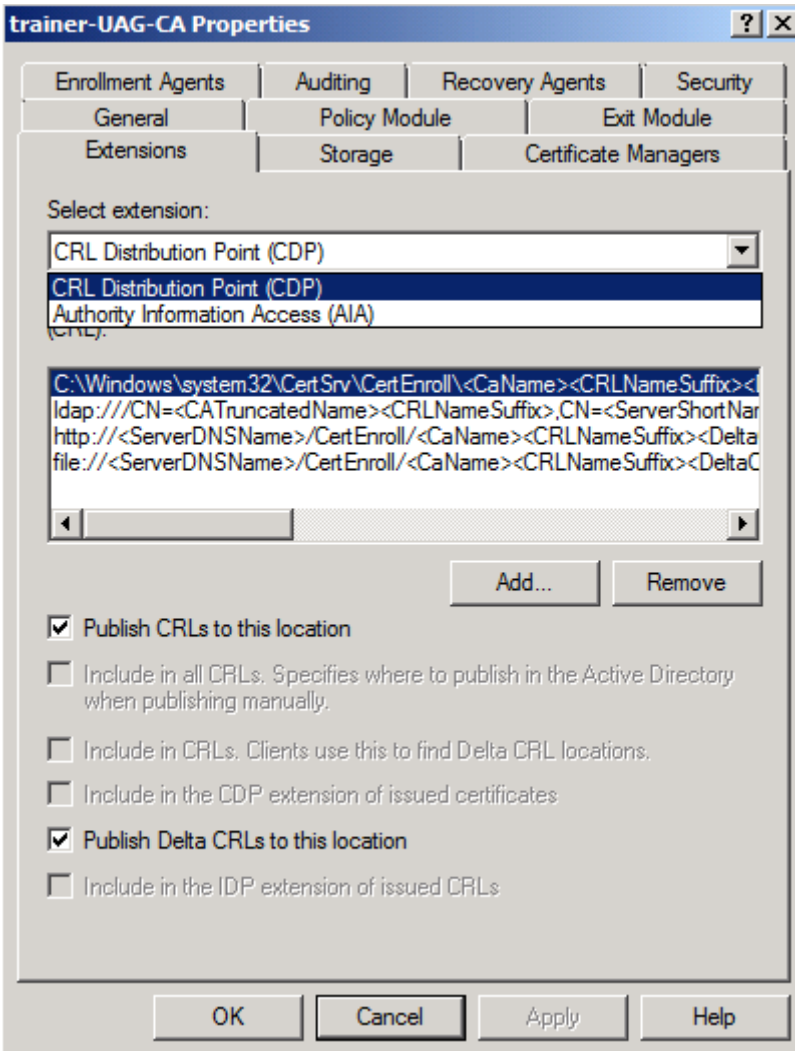

Figure 2: CRL Distribution point

The problem begins when there are domain joined clients such Notebooks, which are connected to the Internet and must check certificates for revocation. Because by default the CDP only contains the internal URL of the issuing CA, a certificate revocation check cannot be done. To overcome this limitation you can modify the CDP with a HTTP location which contains a public URL. With the help of Forefront TMG it is possible to publish the CRL to the Internet. A CRL publishing is a Standard Webserver publishing rule with Forefront TMG. Later in this article I will show you the high level steps how to publish the CRL wit Forefront TMG.

As the next step we must extend the CDP of the CA with a public URL which must be reachable from the Internet with the HTTP protocol. There are many ways to extend the CA with a new HTTP CDP but in my opinion one of the best ways is to use a script to modify the CDP. The next screenshot will show you the content of the script

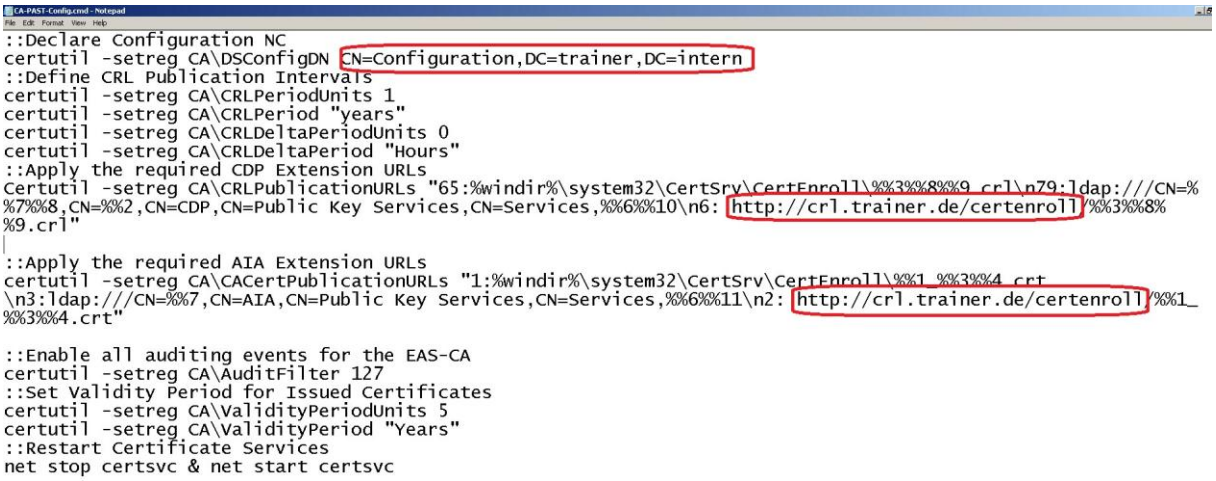

Figure 3: Script to modify CDP and AIA location

You have to change the script with your internal Active Directory Configuration Partition information and the CRL and AIA location. Thanks to Carsten Zuege how gave me access to this script.

OCSP

A detailed description of the OCSP (Online Certificate Status Protocol) is out of the scope of this article but I like to give you some basic informations about the OCSP protocol which can be used as a alternative to the classic CRL publication. The OCSP protocol allows a client to query the status of revoked certificates online against a CA. The CRL must be downloaded by the client as part of a full or delta CRL download. Windows Server 2008 R2 contains a OCSP Responder, as shown in the following screenshot.

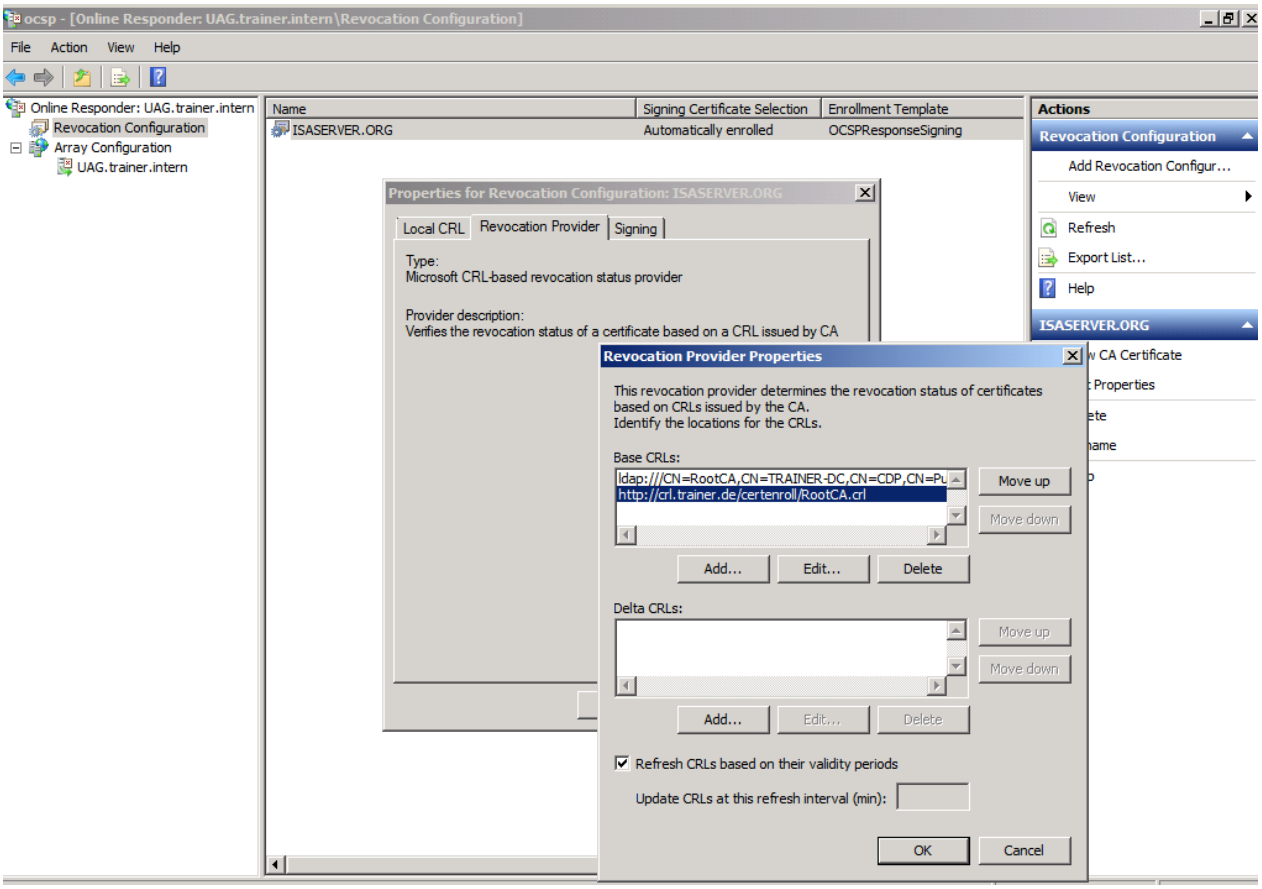

Figure 4: OCSP configuration

CRL publishing with Forefront TMG

Now we can start configuring Forefront TMG to publish the internal CRL to the Internet. We are using the Website Publishing rule wizard. I will only show you the most important steps in the publishing wizard.
First, we must give the publishing rule a name and allow the connection. We are publishing a single website or load balancer. Because a CRL is accessed via a non-encrypted HTTP connection, we only use HTTP.

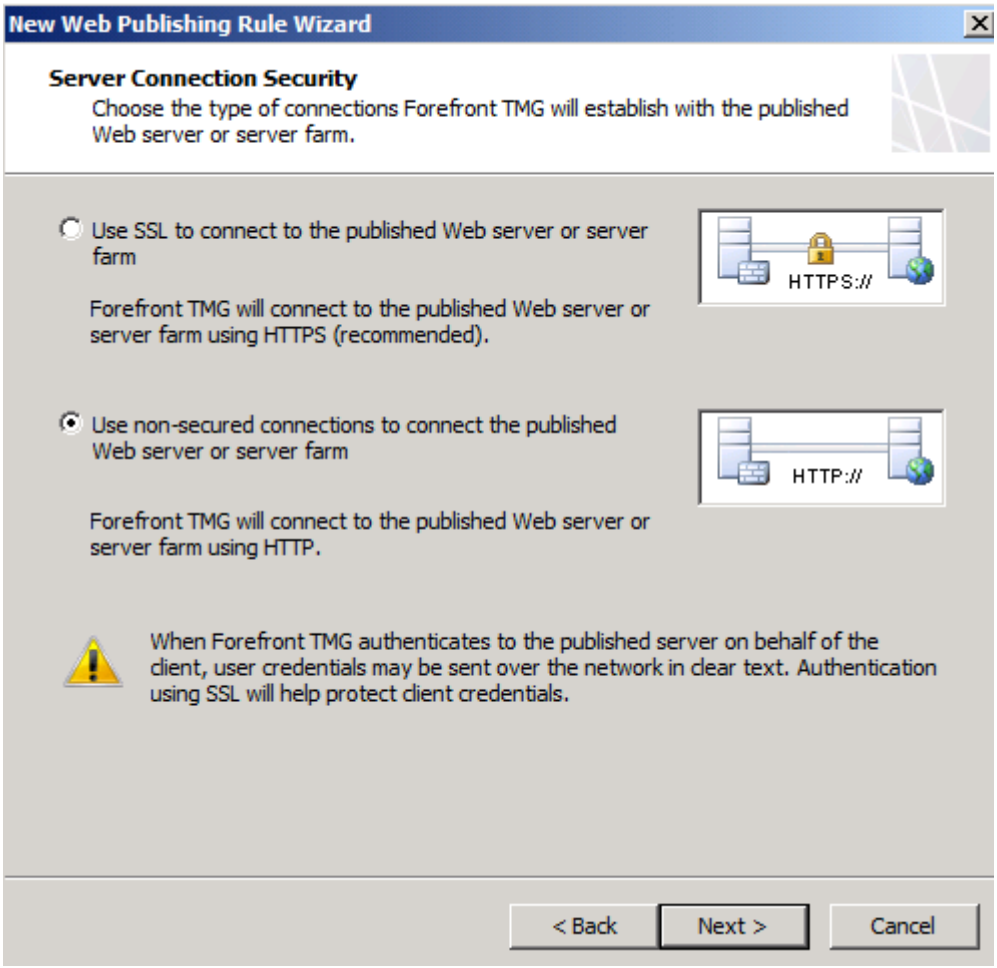

Figure 5: HTTP Webserver publishing

Next, enter the FQDN of the internal CA Server in the wizard. The path to publish is the /Certenroll directory on the IIS of the CA server.

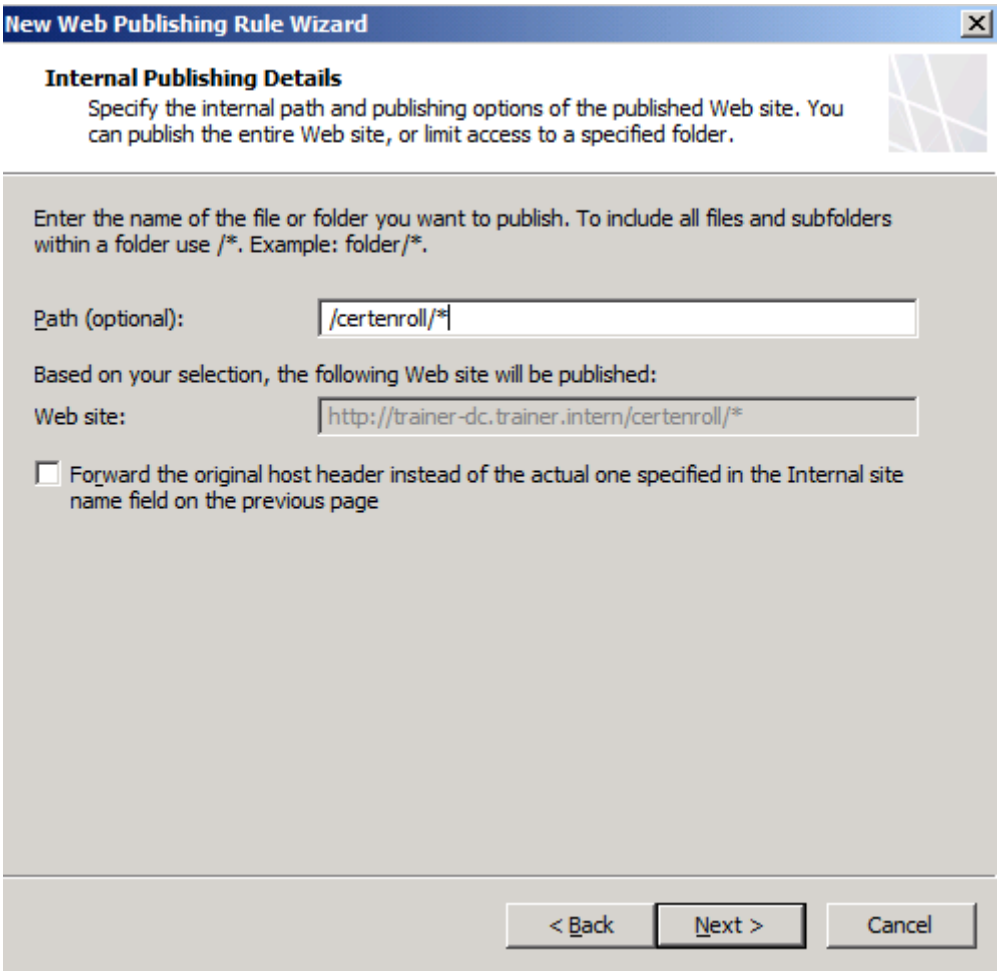

Figure 6: CRL publishing path

Please note: We will restrict access to the required path after the wizard has been finished.

We will accept requests for the public name which you entered previously as a CRL path in the CDP location of your CA server. In this example the CRL will be published to CRL.TRAINER.DE.

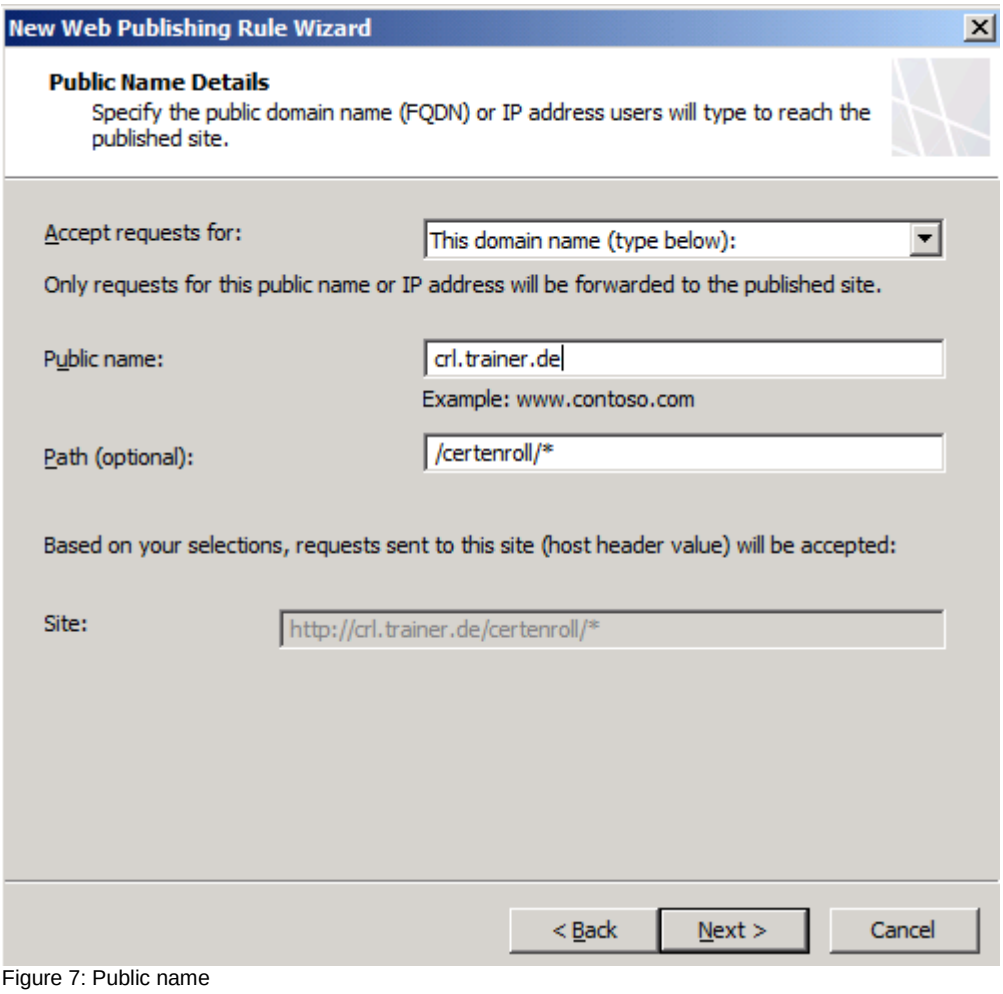

Figure 7: Public name

Next we must create a new weblistener which accepts HTTP connections.

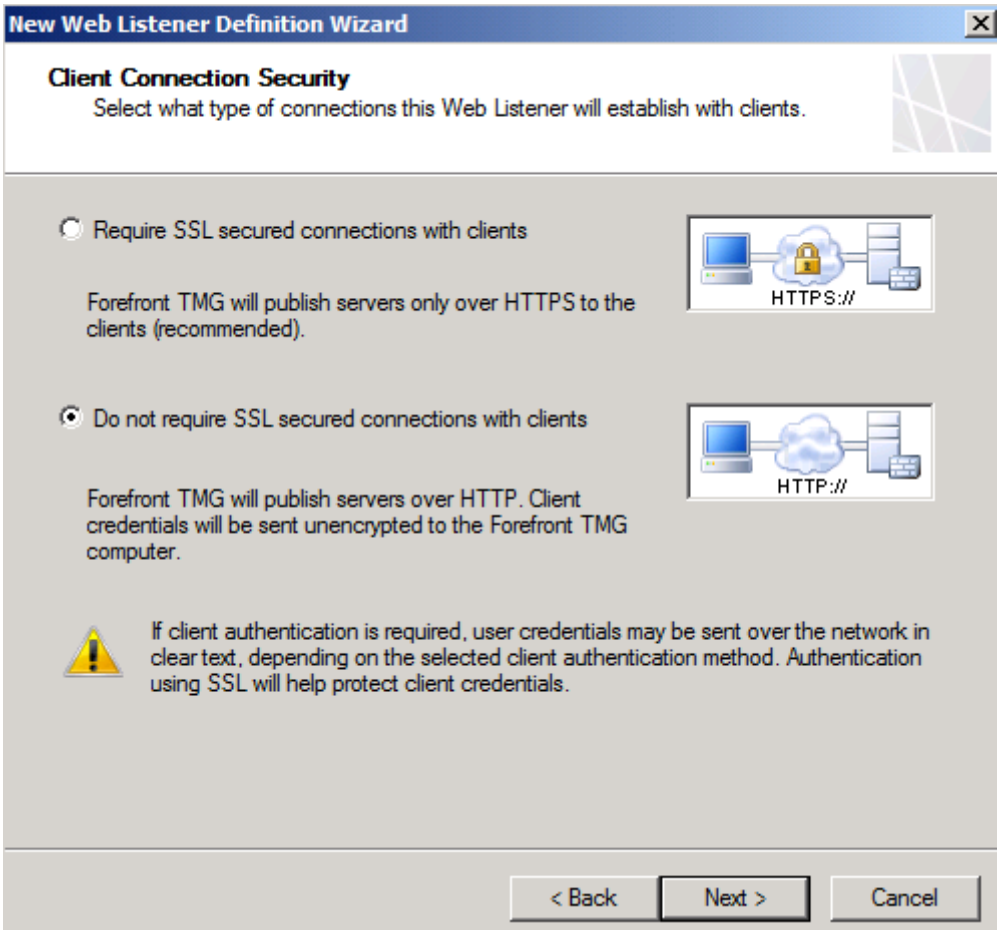

Figure 8: Connect via HTTP

Select the network EXTERNAL or a specific IP address of the external network and select *No authentication*.
Because no authentication is required we select *No delegation, and client cannot authenticate directly* in the authentication delegation window.

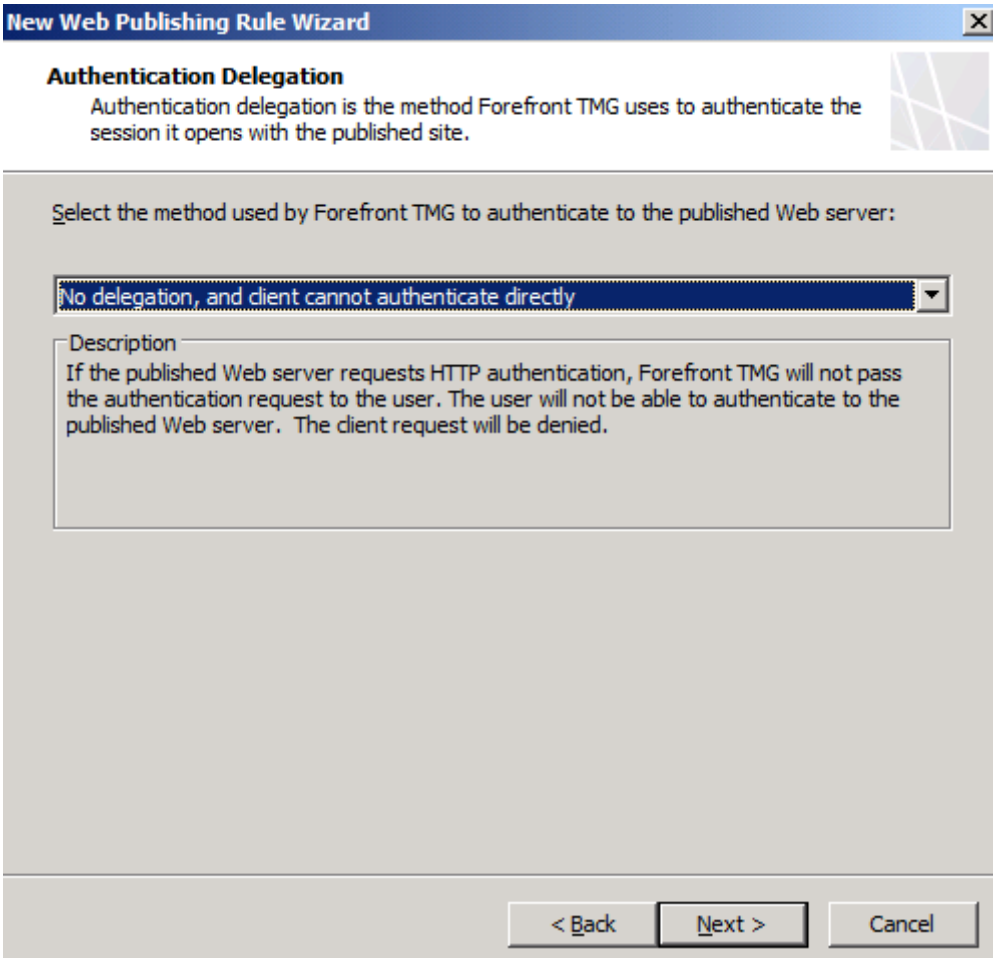

Figure 9: No Authentication delegation

The rule accepts access for *All Users*. Click *Finish* to end the publishing wizard and after that click *Apply* to save the configuration.
After the publishing rule has been created, open the publishing rule, navigate to the *Path* tab and restrict the path to the full path for downloading the CRL as shown in the following screenshot.
Attention: You have to change the path to your current CA configuration. In my example the CA has the name RootCA, so the CRL file is called RootCA.CRL and RootCA+.CRL.
Attention: If your clients need access to download the RootCA+.CRL file, it might be necessary to allow double byte encoding in the web.config file on the IIS Server of the CA.

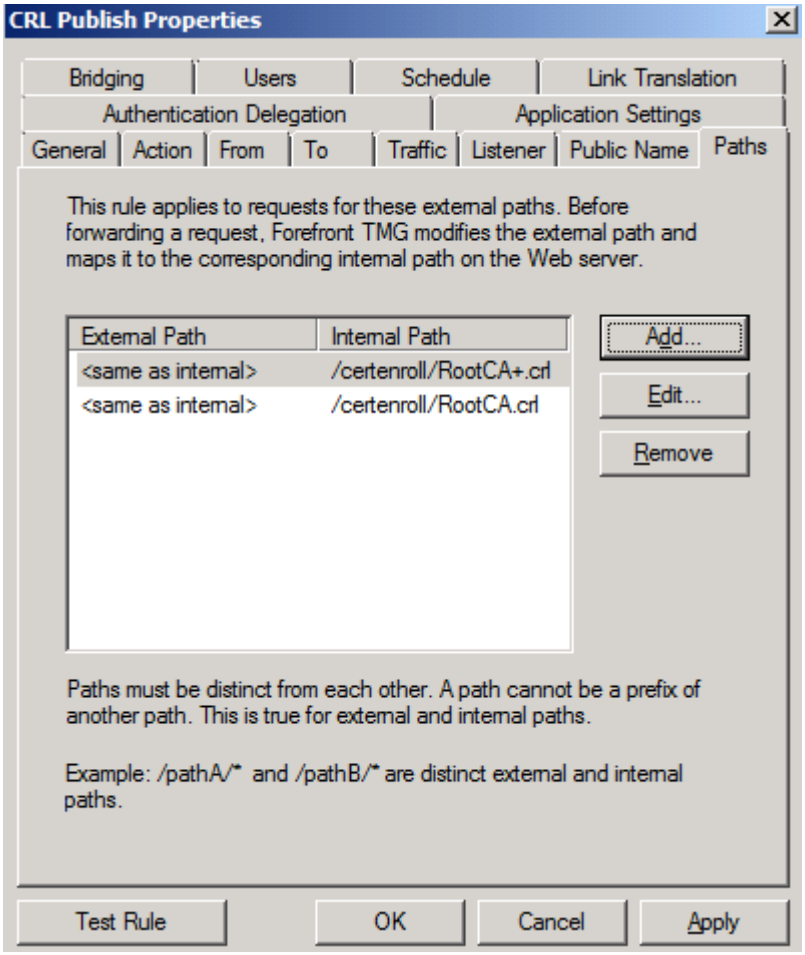

Figure 10: Restrict the path to the CRL

Test the CRL download from an Internet client. Enter the path to the CRL into your Web browser and now it should be possible to download the CRL.

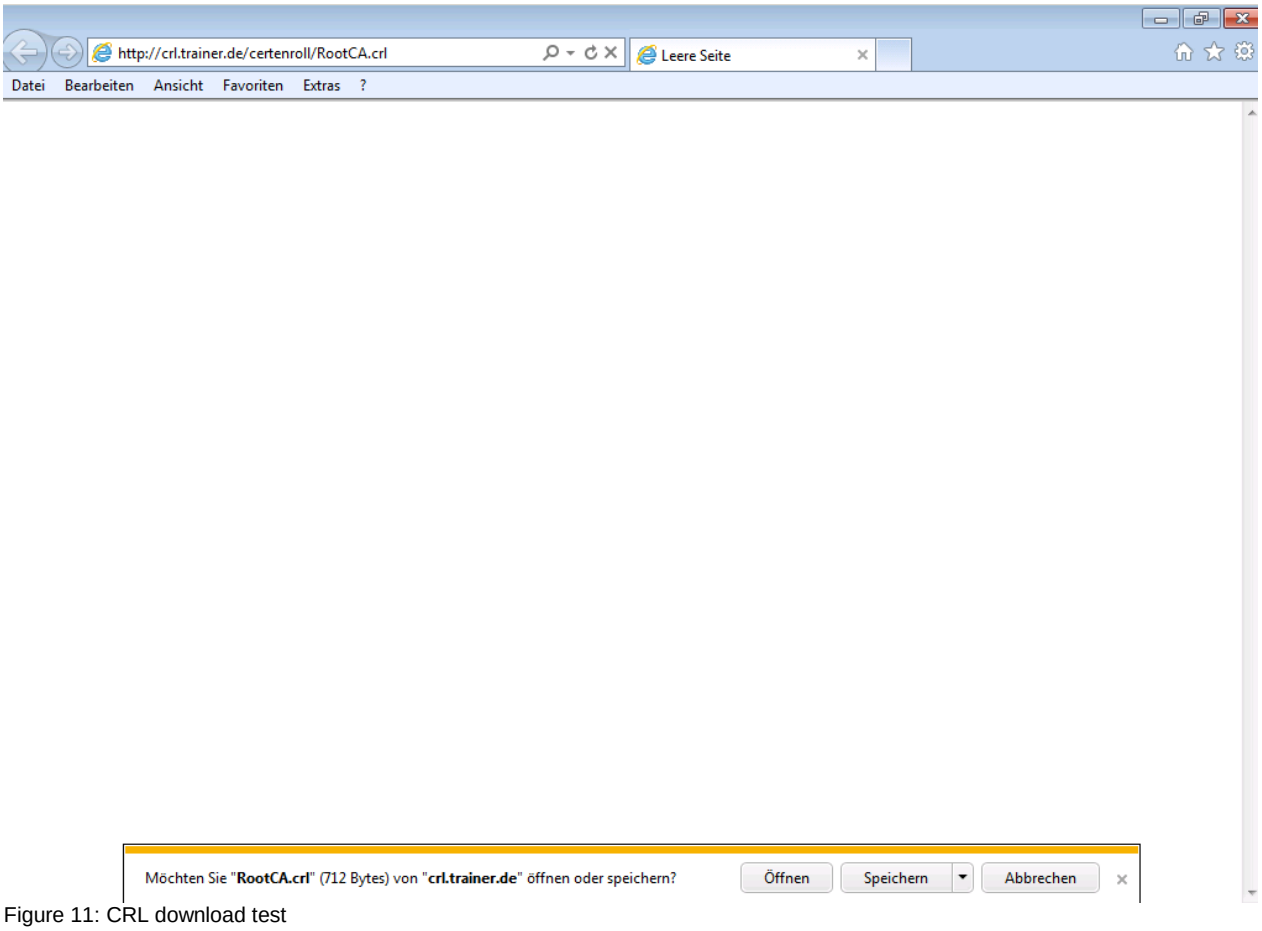

Figure 11: CRL download test

HTTP-filter

You can use the HTTP-filter in Forefront TMG to provide some additional security for the CRL publishing rule. For this example I restricted the maximum URL and URL query length to 256 Byte and the maximum header length to 513 bytes.
Attention: These settings will depend on your current environment, so you have to play with these settings.
Important:
The HTTP Filter in Forefront TMG is rule specific except the Maximum Header length setting. The maximum Header length in Forefront TMG is the same for all Firewall rules with HTTP protocol definitions.
Please note: The maximum header length must be greater than the sum of the maximum URL and URL query length.

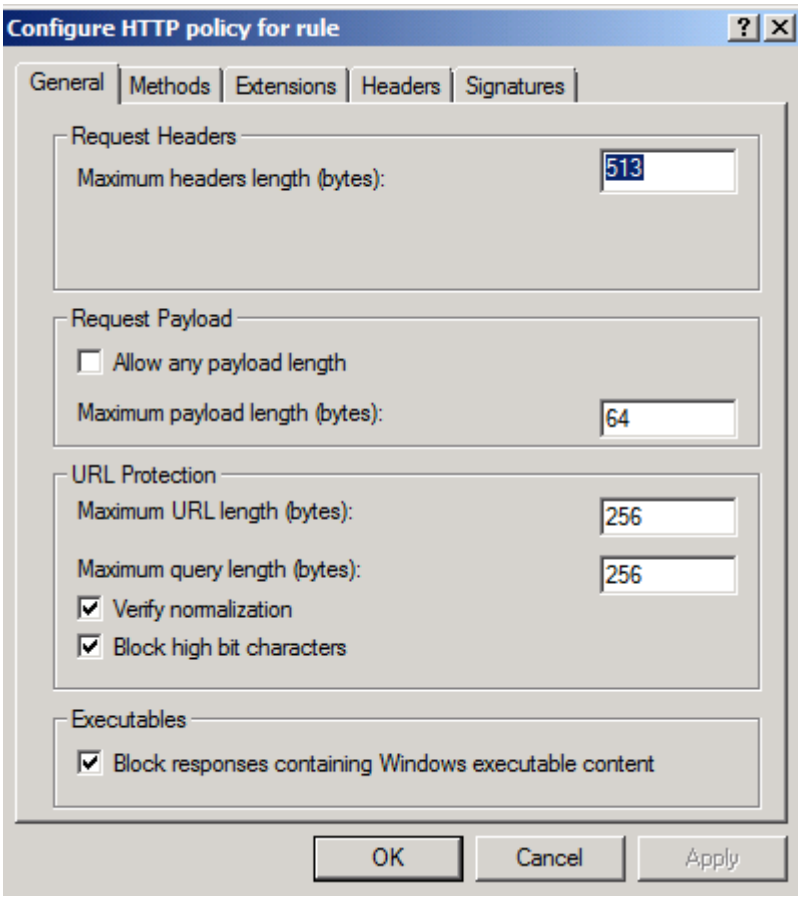

Figure 12: HTTP-filter URL length settings

I also instructed Forefront TMG to block Windows executable content and allowed a maximum payload length of 64 bytes.

If you configure the HTTP-filter to restrictive, you will get an error message like the following.

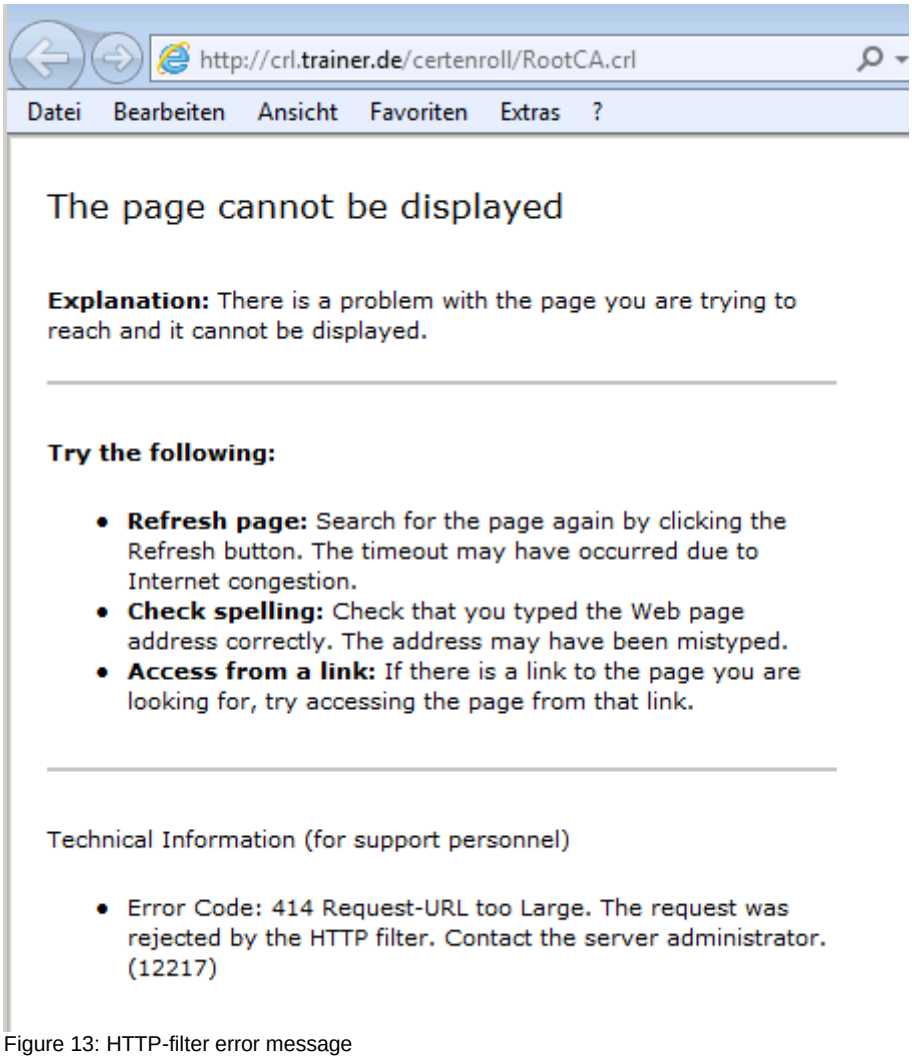

Figure 13: HTTP-filter error message

Because clients will only download the CRL we will allow only the HTTP GET extension.

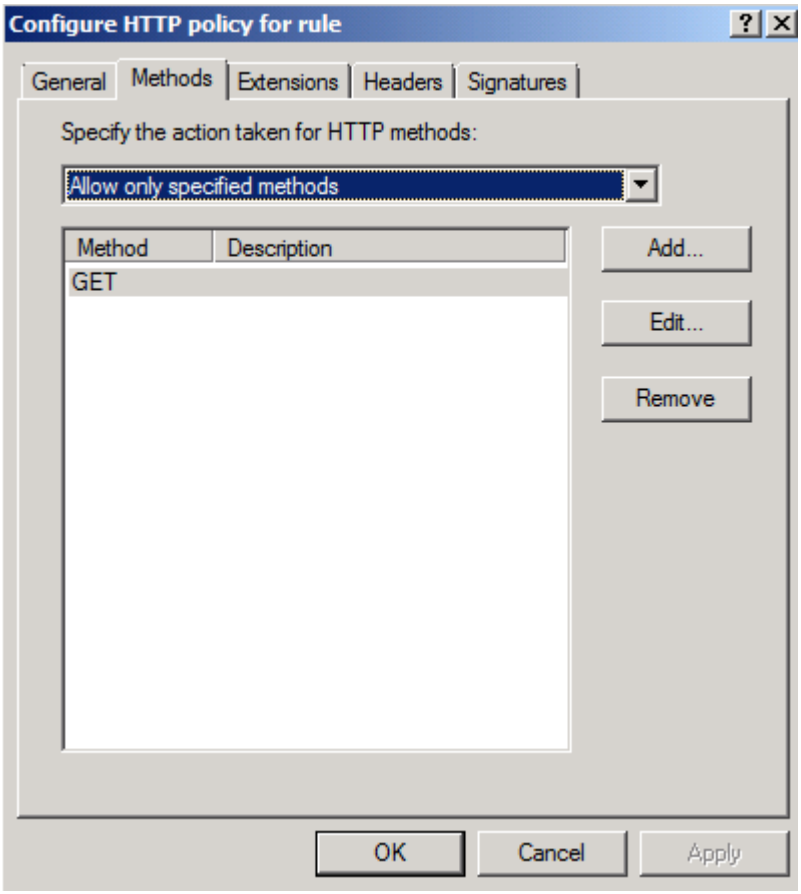

Figure 14: Restrict access to HTTP GET

Next, we configure the HTTP-filter to only allow the .CRL extension to be downloaded.

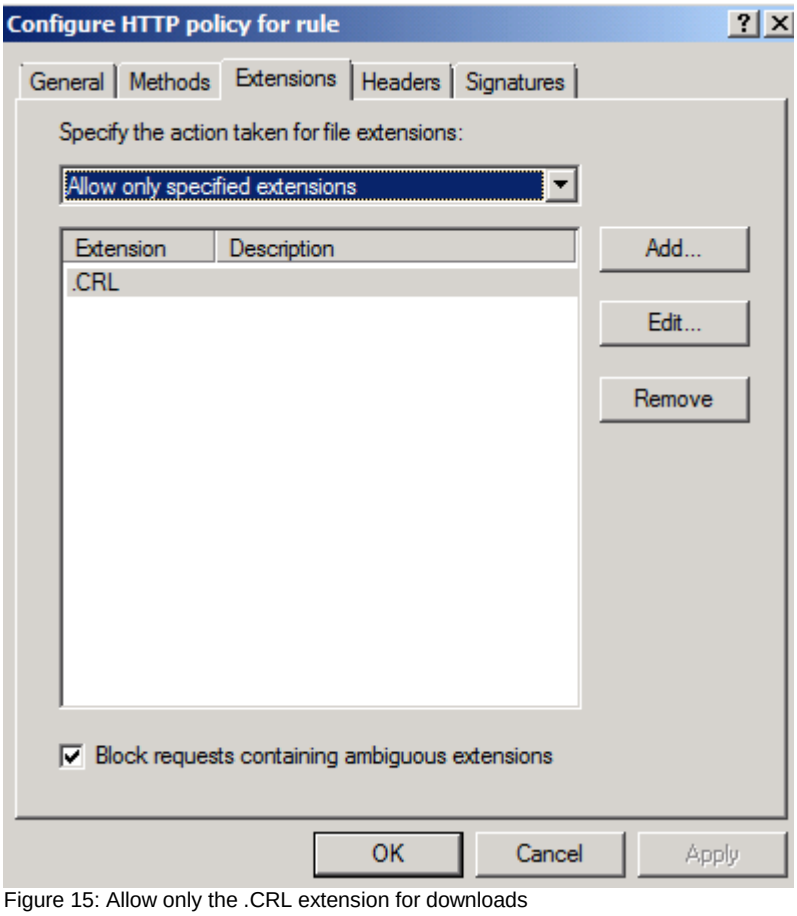

Figure 15: Allow only the .CRL extension for downloads

Conclusion

In this article I tried to give you an overview about Windows certificate services and the process of Certificate revocation with CRL and OCSP. We also had a look how to securely publish a CRL to the Internet with Forefront TMG and the HTTP-filter.

Related links

Microsoft Active Directory Certificate Services
http://www.microsoft.com/PKI/
Configure CDP and AIA Extensions
http://technet.microsoft.com/en-us/library/cc776904(WS.10).aspx
Publishing Certificate Revocation Lists with ISA Server 2006 - Part 1: Creating the Publishing Rule
http://blog.msfirewall.org.uk/2008/06/publishing-certificate-revocation-lists.html
How to configure Certificate Services and ISA Server to publish CRLs
http://support.microsoft.com/kb/318707
Publishing a Public Key Infrastructure with ISA Server 2004 (Part 1)
http://www.isaserver.org/tutorials/Publishing-Public-Key-Infrastructure-ISA-Server-2004-Part1.html
How to Configure UAG to Publish Your Private Certificate Revocation List
http://blogs.technet.com/b/tomshinder/archive/2010/08/03/how-to-configure-uag-to-publish-your-private-certificate-revocation-list.aspx
Configure a CA to Support OCSP Responders
http://technet.microsoft.com/en-us/library/cc732526.aspx
Configuring the Forefront TMG HTTP Filter

http://www.isaserver.org/tutorials/Configuring-Forefront-TMG-HTTP-Filter.html