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

Certificate requirements for Forefront TMG and UAG

Abstract

This article will show you the requirements for certificates in Forefront TMG and UAG publishing scenarios, VPN connections and high available configurations.

Let's begin

Using certificates in Forefront TMG and UAG is for many Administrators a complex process because they must work rarely with Server and client certificates, certificate authorities and certificate revocation configurations. Forefront TMG and UAG makes massive use of certificates in different publishing, VPN and authentication scenarios, so it is essential to have a good understanding about how certificates work in general and how they are used in Forefront TMG and UAG.

Type of certificates

Let use first talk about the different certificate types. There are three certificate types:

- Single Name certificate
- Wildcard certificate
- SAN (UCC) certificate

A single name certificate is a certificate with only one DNS name in the common name (CN) field of the certificate. For example, there is a certificate issued to www.isaserver.org. This certificate can be used to publish internal websites with Forefront TMG and UAG and when users type http://www.isaserver.org in theirs web browsers everything is fine and no certificate error appears. If the user types the public IP address assigned to the host www.isaserver.org he will get an error message that the name of the certificate doesn't matches the name entered in the web browser.
A wildcard certificate is a certificate issued to a DNS domain name, for example *.isaserver.org. With this certificate it is possible to publish different Servers to the Internet for example ftp.isaserver.org and www.isaserver.org without getting a certificate error message.
A SAN (Subject Alternate Name) or UCC (Unified Communication Certificate) is a certificate which may contain FQDN from different domains for example www.isaserver.org, www.msexchange.org and more. This certificate type is often used in Microsoft Lync and Microsoft Exchange Server publishing's.
Please note: There are also special UCC/SAN certificate which may also contain wildcard names.

Certificate validation

During the certificate validation process of different applications and web browsers, the validation process checks if the certificate has been issued from a trusted Root certification authority. The validation process looks into the certificate store of the

local computer in the Trusted Root CA store. If the certificate is self-signed or has been issued from an internal Windows CA (Certificate Authority), a warning message will appear that the certificate is not trusted if the client computer is not member of the Active Directory forest where the CA exists.

During the certificate validation process, many applications and web browsers also checks if the certificate hasn't been revoked. The validation process checks the certificate Distribution Point (CDP) in the certificate and tries to download the CRL or to check online again revocation when OCSP is used.

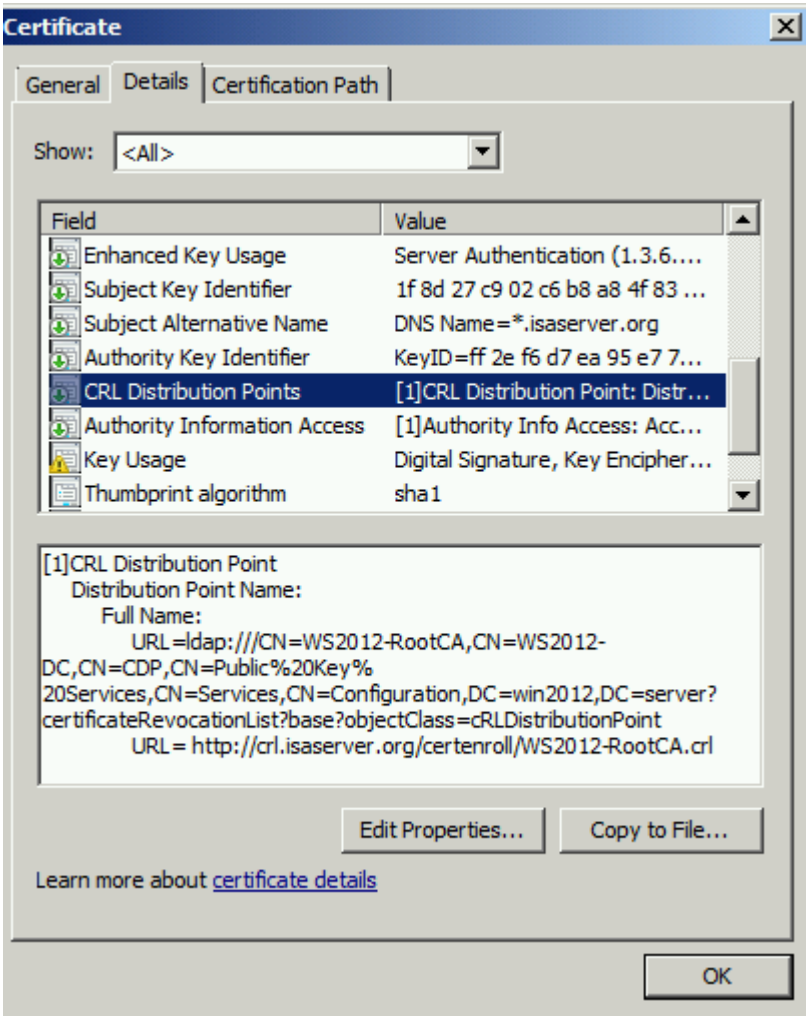

Figure 1: CRL Distribution Points

Forefront TMG can also be configured to check certificates in forward or reverse scenarios against revocation. It is possible to configure this TMG behavior in the TMG MMC in the Web Access Policy node as shown in the following picture.

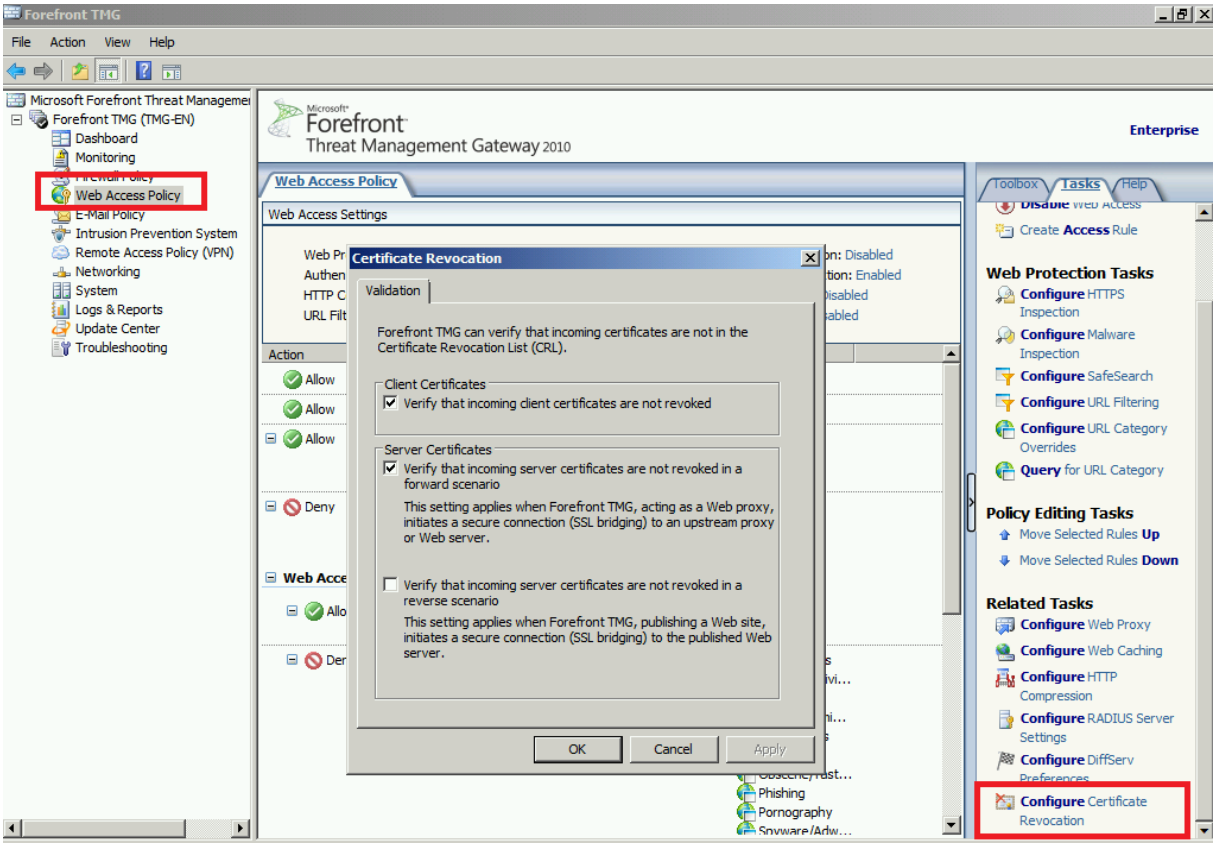

Figure 2: Certificate revocation

Certificate stores

Every Windows Operating system has a certificate store to store personal certificate for the local computer account, user or service accounts. The certificate store also contains certificates from Trusted Root Certification Authorities. To open the certificate store you can use command line tools or a MMC. Start en empty MMC and add the certificate SnapIn as shown in the following picture.

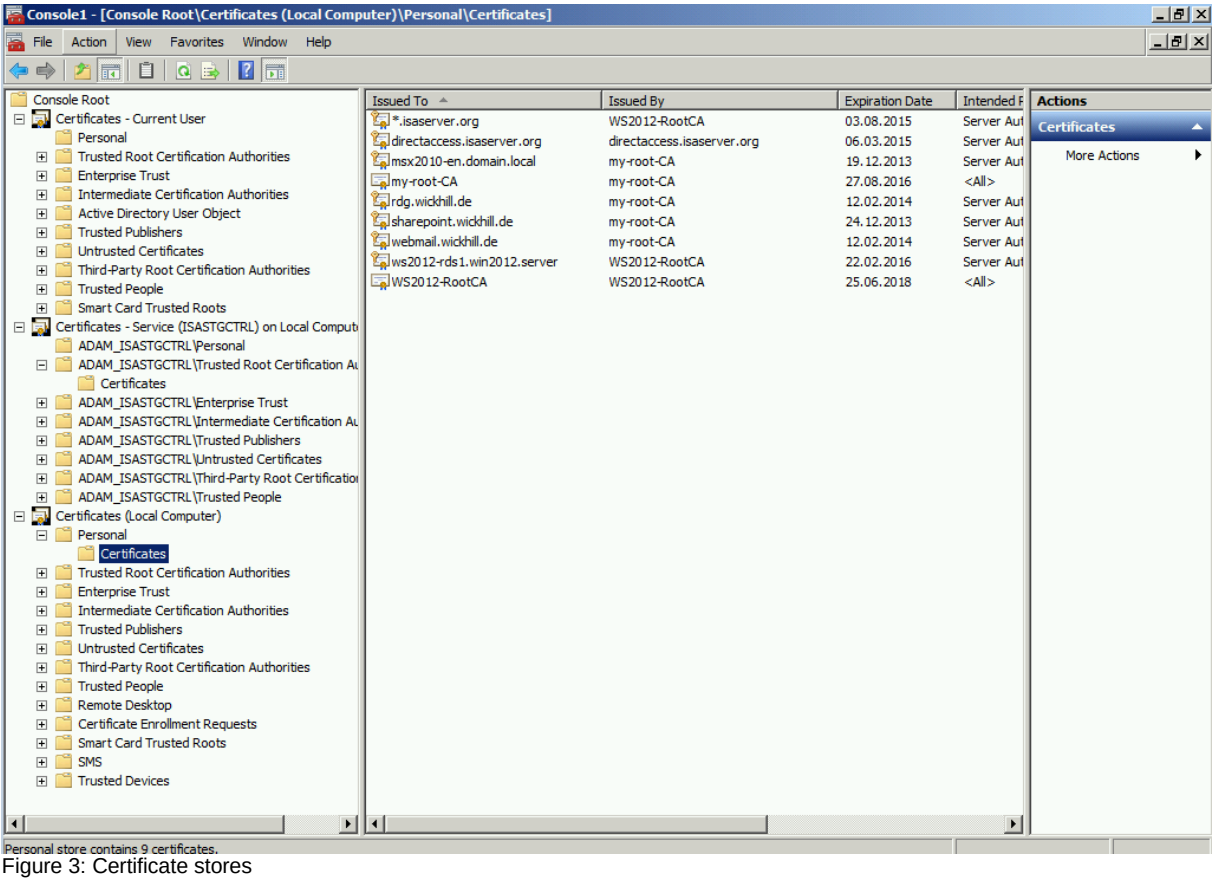

Figure 3: Certificate stores

The correct certificate store location is important if you use Forefront TMG and UAG. Typically certificate must be stored in the certificate store of the local computer. In rare scenarios certificates must also be placed in the certificate store for a Windows service like the Forefront TMG ISASTGCTRL service as shown in the picture above.

Certificates in Web Listeners

If you create a secure Webserver publishing rule in Forefront TMG you must create a Web listener. The Web listener is used by Forefront TMG to listen for web requests from clients on the Internet. Tis Web listener must be configured with a certificate with the following requirements:

- Stored in the Computer certificate store
- Certificate has been issued from a trusted Root CA
- Contains a valid name (Single Name, Wildcard, UCC/SAN) in the certificate used by the public name in the publishing rule

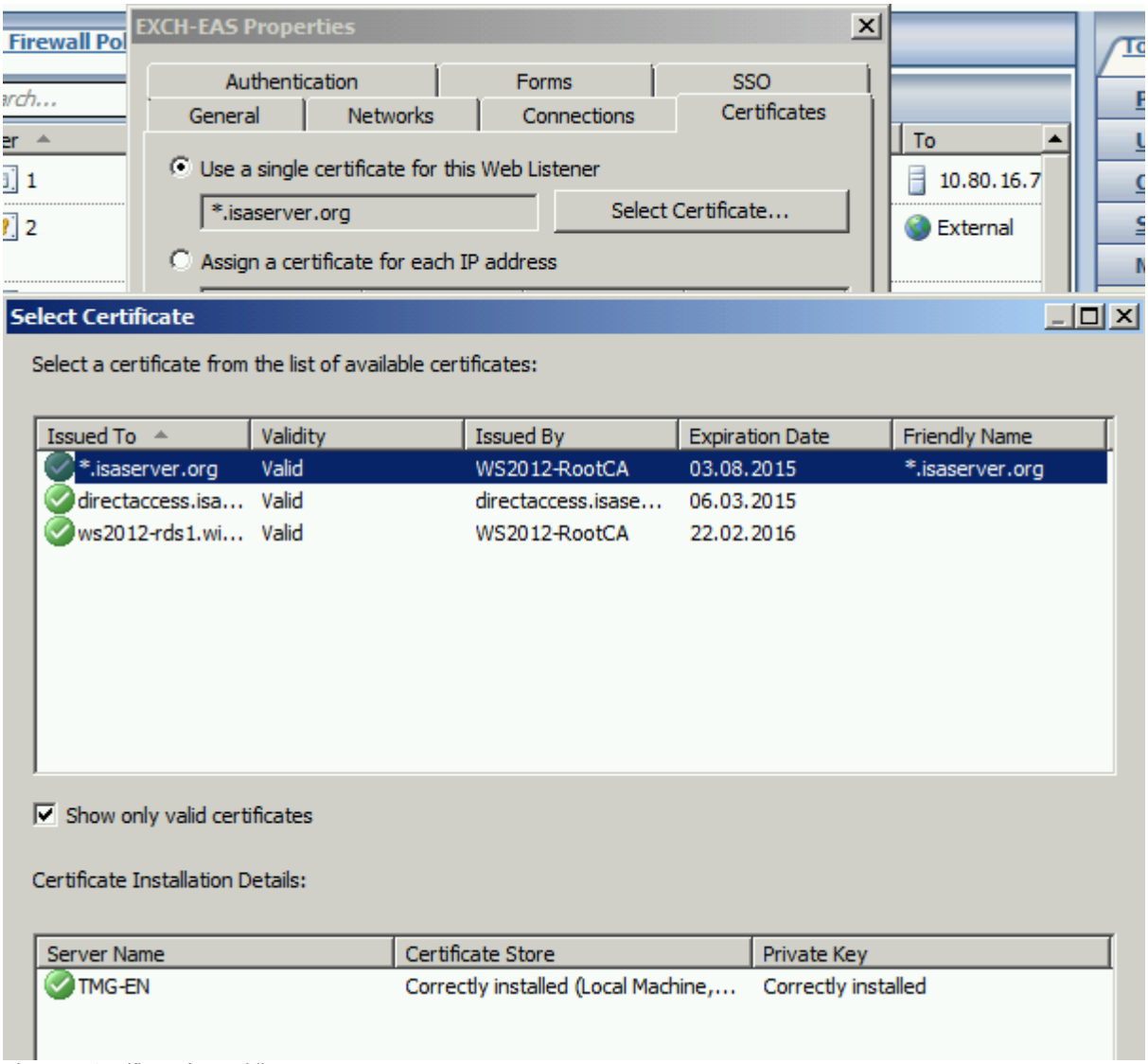

Figure 4: Certificate for Weblistener

Forefront TMG/UAG administrators have options to limit the use of Certificate Authorities or Client certificate restrictions in the advanced authentication options in the publishing rule as shown in the following picture.

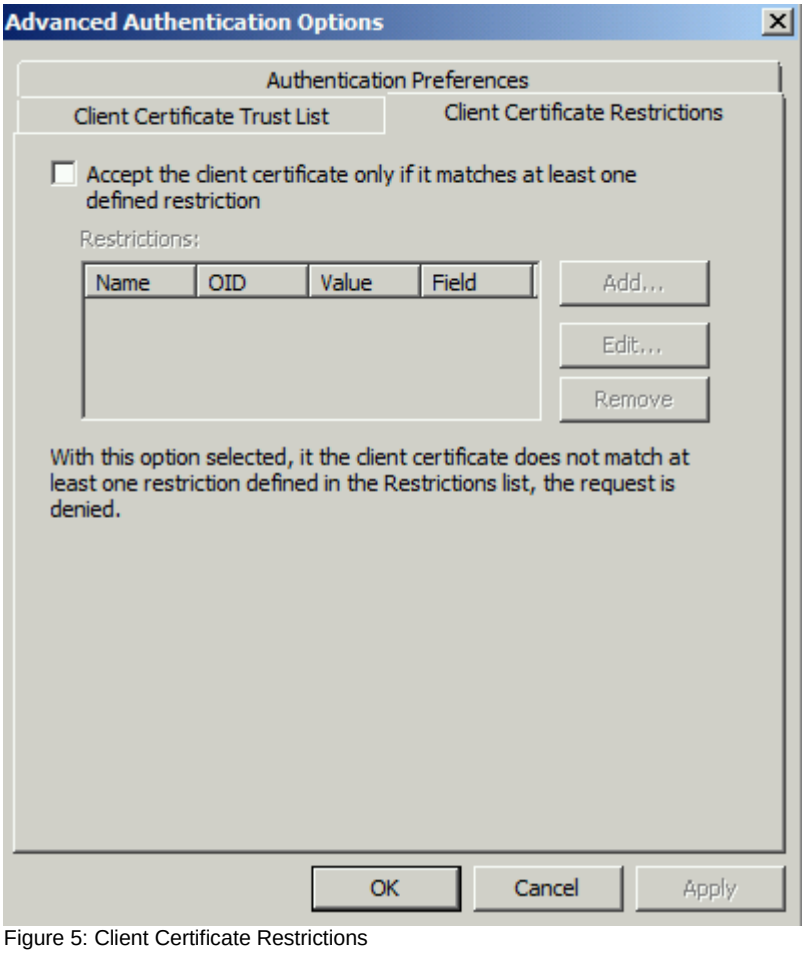

Figure 5: Client Certificate Restrictions

A special configuration setting can be found in properties of the publishing rule on the Bridging tab.
The option is called “use a certificate to authenticate to the SSL Web Server”. Many Administrators are confused when to use this option. This option must only be used in a HTTPS to HTTPS bridging scenario when the published Webserver requires SSL client certificate authentication. Because Forefront TMG terminates the SSL request from the client on the Internet and establishes a new SSL connection to the published webserver, Forefront TMG becomes a SSL client and must authenticate against the internal Webserver with a SSL client certificate.

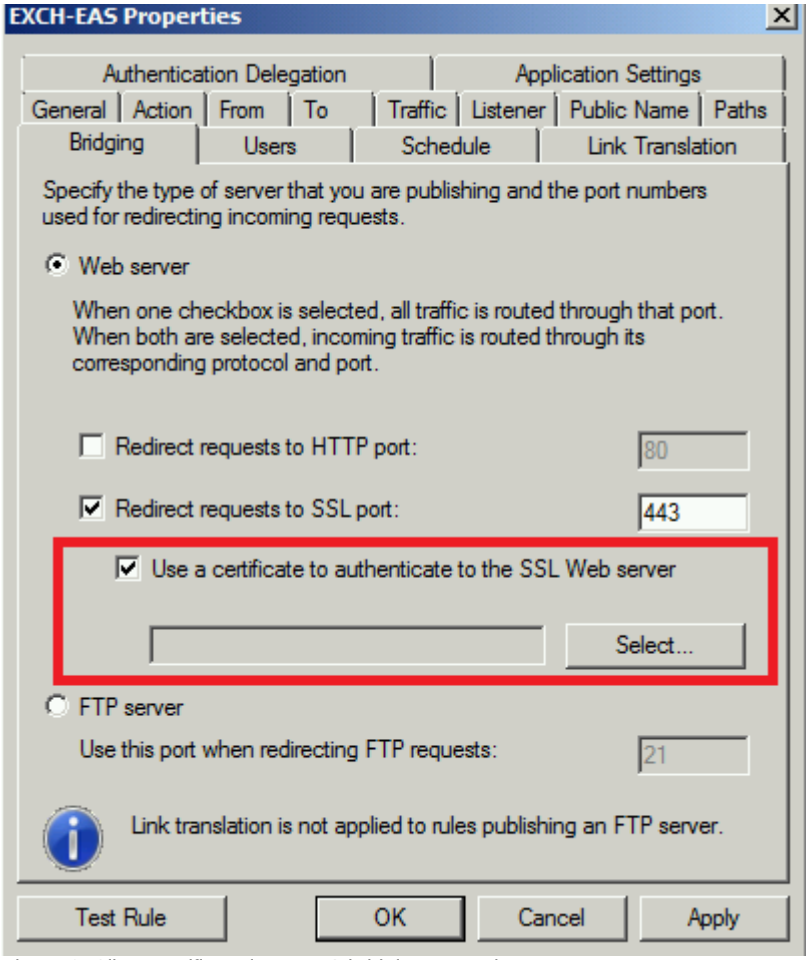

Figure 6: Client certificate in HTTPS bridging scenarios

SSL client certificates

Forefront TMG can be configured for SSL Client Certificate authentication. A client on the Internet must have a certificate stored in the certificate store of the user or computer depending on the type of SSL Client certificate authentication. Forefront TMG uses this certificate to authenticate the user or computer.

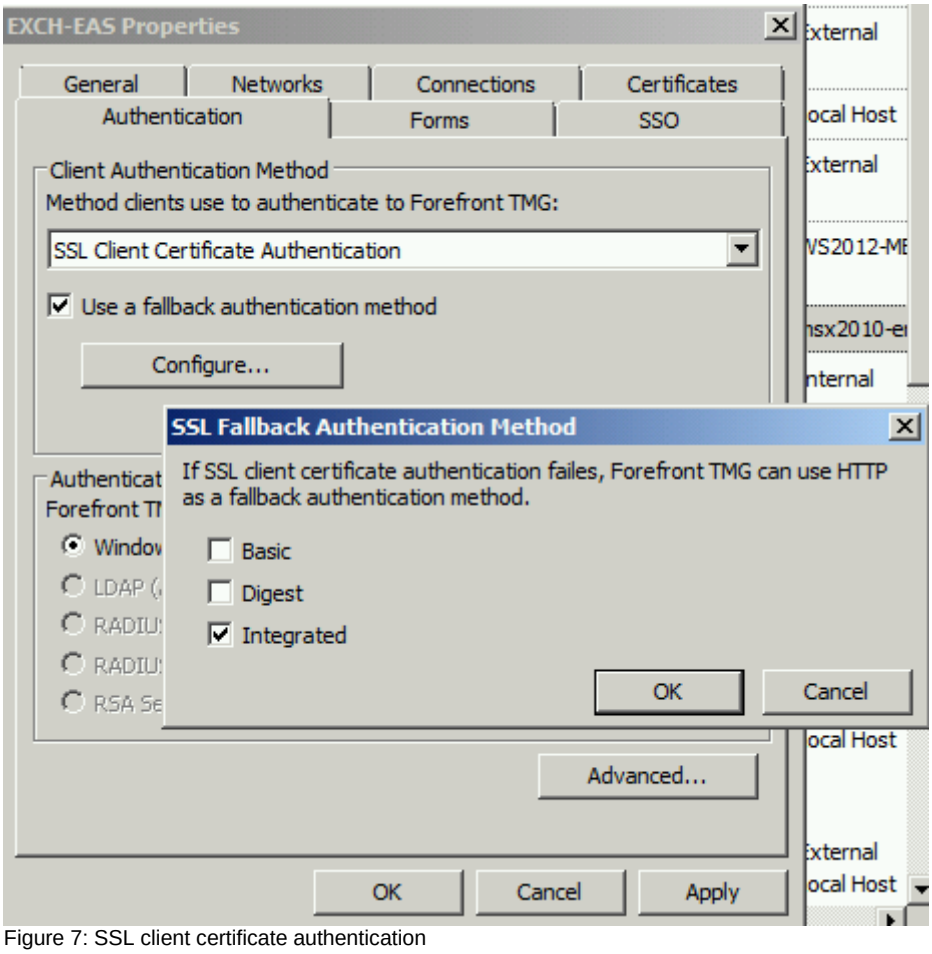

Figure 7: SSL client certificate authentication

A Fallback can be configured if a certificate is not present.

Certificates in TMG/UAG arrays

A Forefront TMG/UAG array can be configured for certificate based communication if the array members are part of a workgroup. More information about this process can be found in this article published on www.isaserver.org.

Forefront UAG portal

Publishing Web Servers in Forefront UAG is done with a Forefront UAG portal trunk and applications in this trunk. A trunk is like a Web Listener in Forefront TMG and must be configured with IP addresses and if a HTTPS trunk has been created with a valid certificate as shown in the following picture.

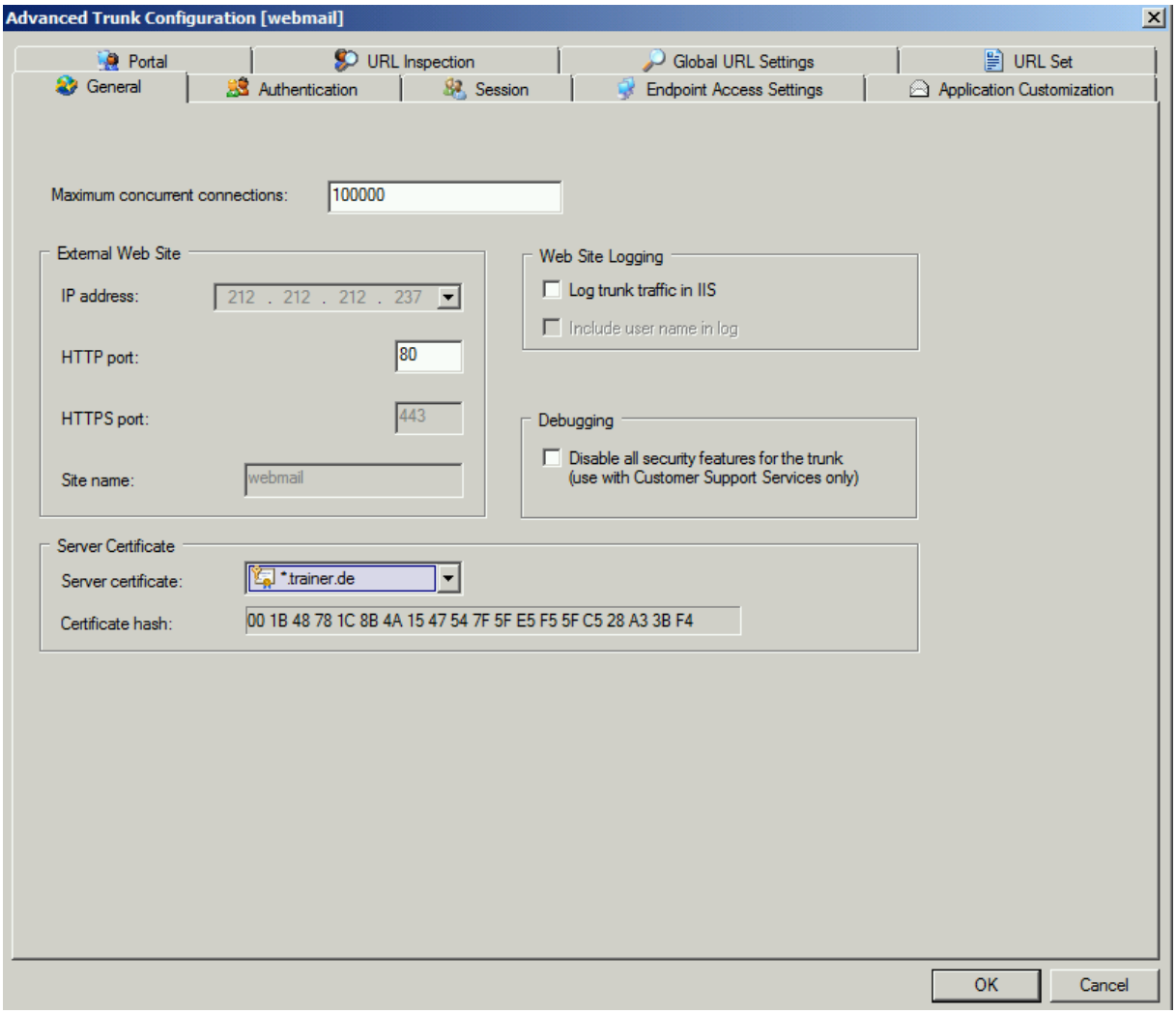

Figure 8: Certificates in Forefront UAG portal trunks

Error message certificate principal name is wrong

In the public ISA/TMG newsgroups or now in the Microsoft Technet forum I often heard about TMG and UAG Administrator who gets the error message „500 Internal Server Error – The target principal name is incorrect" when users try to access a published Webserver on the Internet. This message has nothing to do with the certificate bound on the Web Listener on the TMG Server. In a HTTP(S) to HTTPS bridging scenario, Forefront TMG terminates the SSL channel between the client on the Internet and the TMG Server and creates a new SSL channel from the TMG Server to the published web server. If the published web server has a certificate bound on the web server with a different CN as entered in the TMG publishing rule on the "To" tab, this error occurs. Forefront TMG/UAG Administrators must make sure that the name in the publishing rule matches the names in the certificate on the published web server. The following picture shows the TMG publishing rule an.

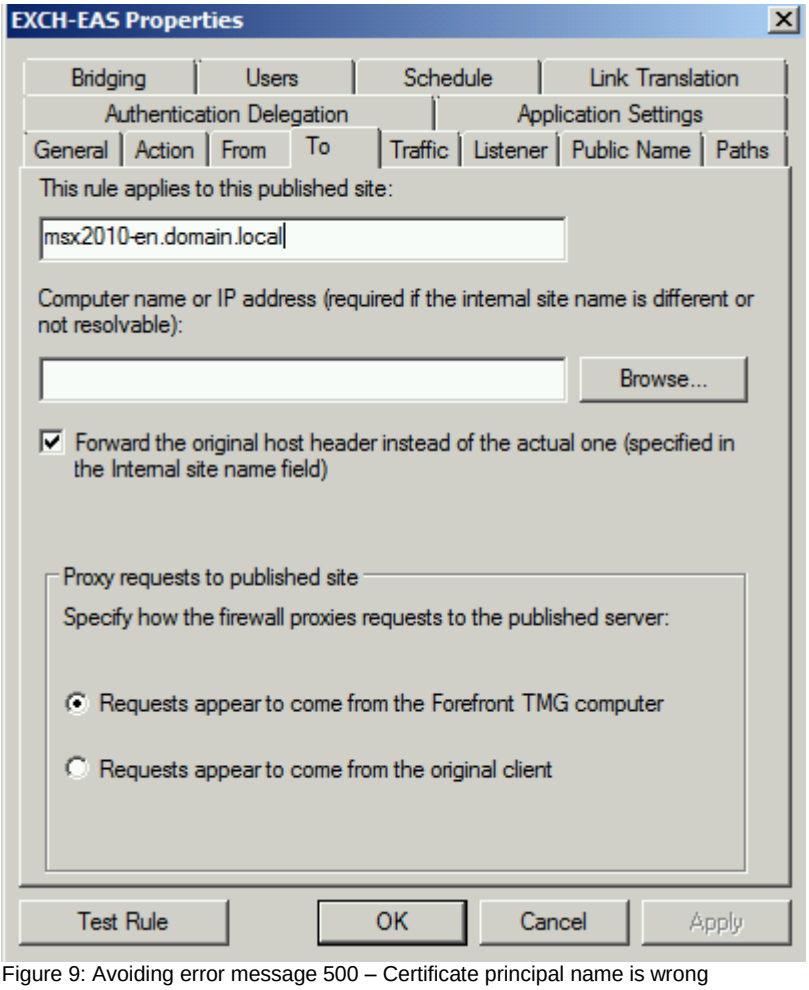

Figure 9: Avoiding error message 500 – Certificate principal name is wrong

HTTPS inspection

Forefront TMG has the capability to inspect outgoing HTTPS traffic. TMG works as a man in the Middle and establish a SSL connection to the desired destination website instead of the client. With this configuration Forefront TMG is able to look into the HTTP packets to enforce corporate compliance. TMG Administrator have to ways to create the HTTPS inspection certificate. First TMG can create a self-signed certificate for HTTPS inspection. This certificate will be distributed via Group Policy to every domain joined client to avoid the certificate error message, that the connection to the destination website is not trusted. TMG Administrators can also use an existing certificate from a public or internal Certificate Authority. The process of using an existing certificate from an internal certification authority is documented here.

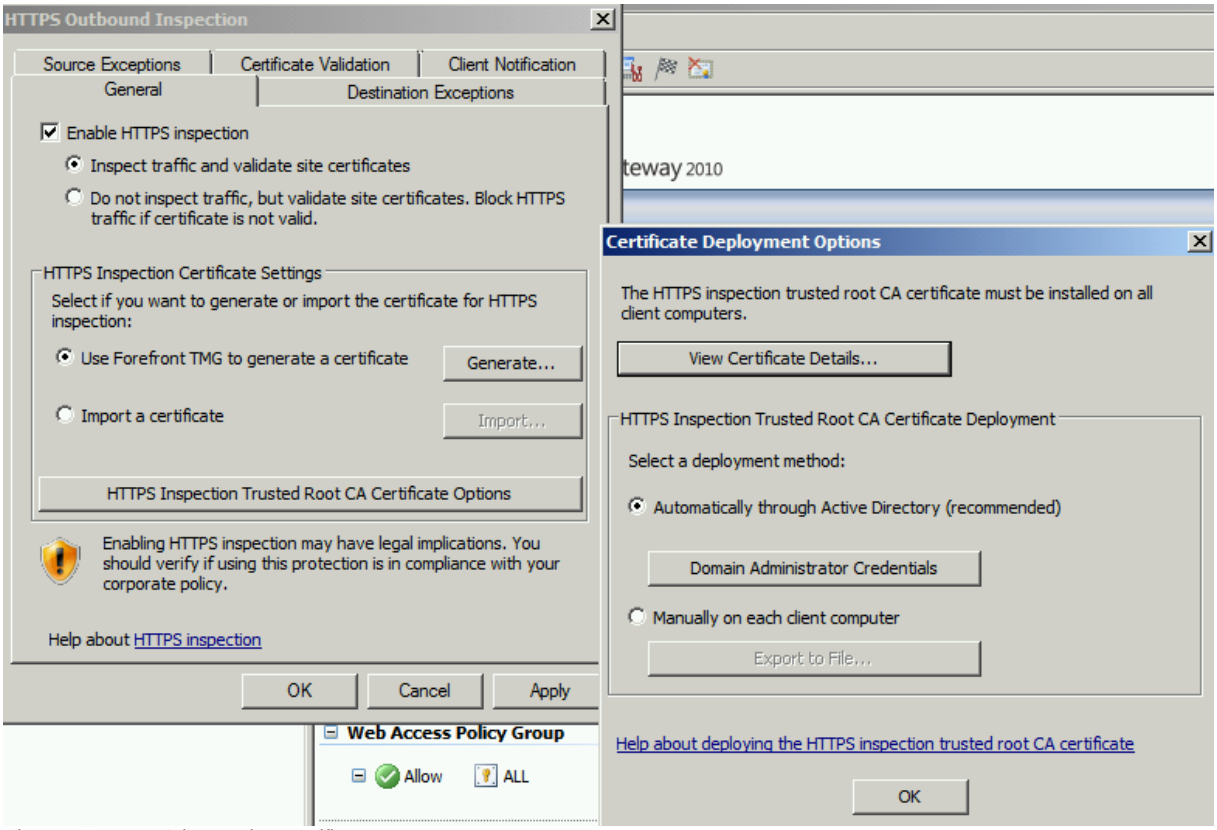

Figure 10: HTTPS inspection certificate

SSTP VPN

Forefront TMG provides VPN clients different access methods to establish a VPN connection. PPTP / L2TP over IPSEC and SSTP (Secure Socket Tunneling Protocol) can be used. If TMG or UAG Administrator configures their Servers for a SSTP VPN connection, they must configure the Web Listener used by SSTP for SSL Client Certificate Authentication and in the Advanced configuration they must make sure that the checkbox “Require SSL Client Certificate” has been enabled. In case of SSTP the CDP of the certificate used by the SSTP Weblistener must be available for SSTP clients on the Internet. Part of the SSTP process is to check if the certificate was issued from a Trusted Root CA and that the certificate hasn’t been revoked. If you use a certificate from an internal CA you must publish the CDP to the Internet. The process is documented for TMG here and for UAG here.

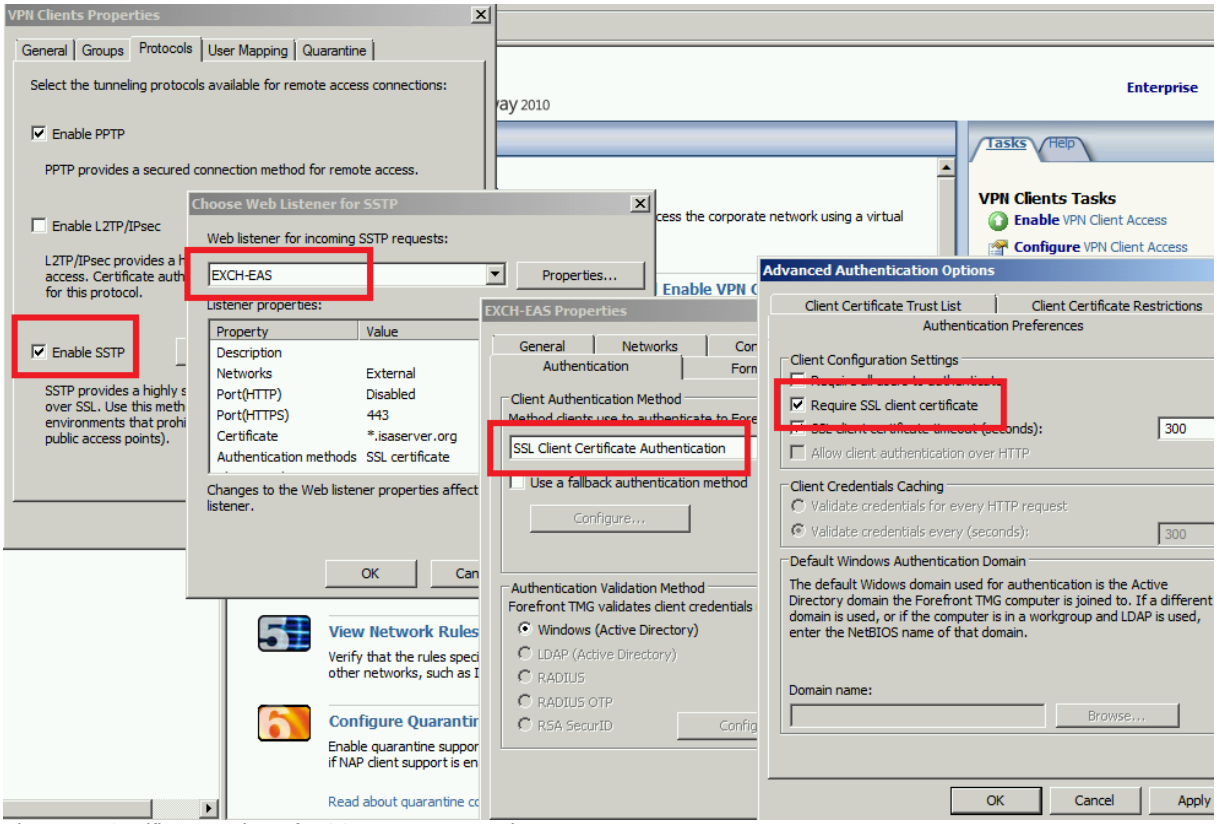

Figure 11: Certificate settimgs for SSTP VPN connections

Conclusion

Using certificates in Forefront TMG and UAG is for many Administrators a complex process because they must work rarely with Server and client certificates, certificate authorities and certificate revocation configurations. In this article I hope that I give you a basic understanding about certificate usages in Forefront TMG and UAG for different publishing, VPN and authentication scenarios.

Related links

Public key certificate
http://en.wikipedia.org/wiki/Public_key_certificate
Authentication in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794722.aspx
Generating the HTTPS inspection certificate
http://technet.microsoft.com/en-us/library/dd441053.aspx
About SSL bridging and publishing
http://technet.microsoft.com/de-de/library/cc995200.aspx
500 Internal Server Error – The target principal name is incorrect
http://technet.microsoft.com/en-us/library/bb794843.aspx