
How to configure Forefront UAG as a SSTP VPN Server

Abstract

In this article I will show you how to use Forefront UAG to provide VPN clients access to internal resources with a SSTP VPN connection.

Let's begin

Forefront UAG offers different VPN option for mobile users. DirectAccess for anywhere access as a permanent VPN connection for domain joined Windows 7 Ultimate and Enterprise clients, SSTP (Secure Socket Tunneling Protocol) for Windows Vista SP1 and higher clients, and the legacy SSL network Tunneling Server for older clients with Windows XP as the operating system.

To configure Forefront UAG as a SSTP Server start the Forefront UAG management console and click *Admin – Remote Network Access – SSL Network Tunneling (SSTP)*.

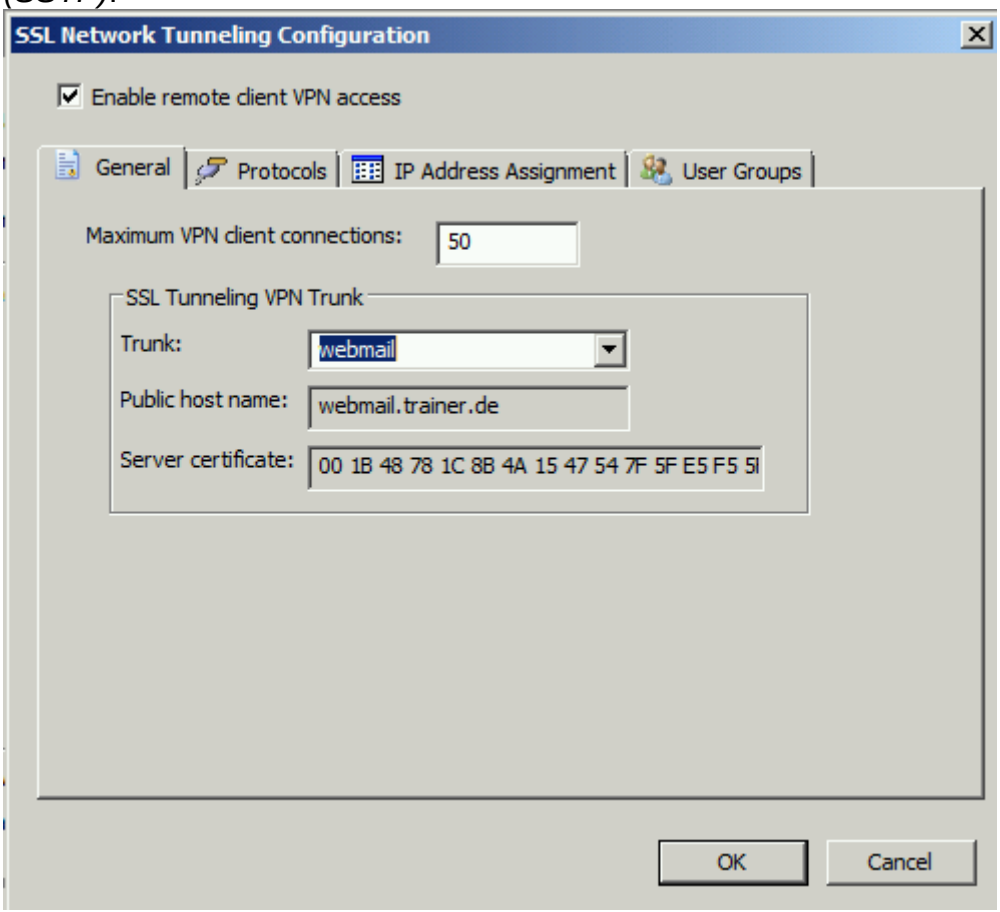

Figure 1: Enable SSTP

Enable remote client VPN access, specify the maximum number of VPN client connections and select the UAG trunk for which SSTP VPN access should be enabled.

SSTP is enabled

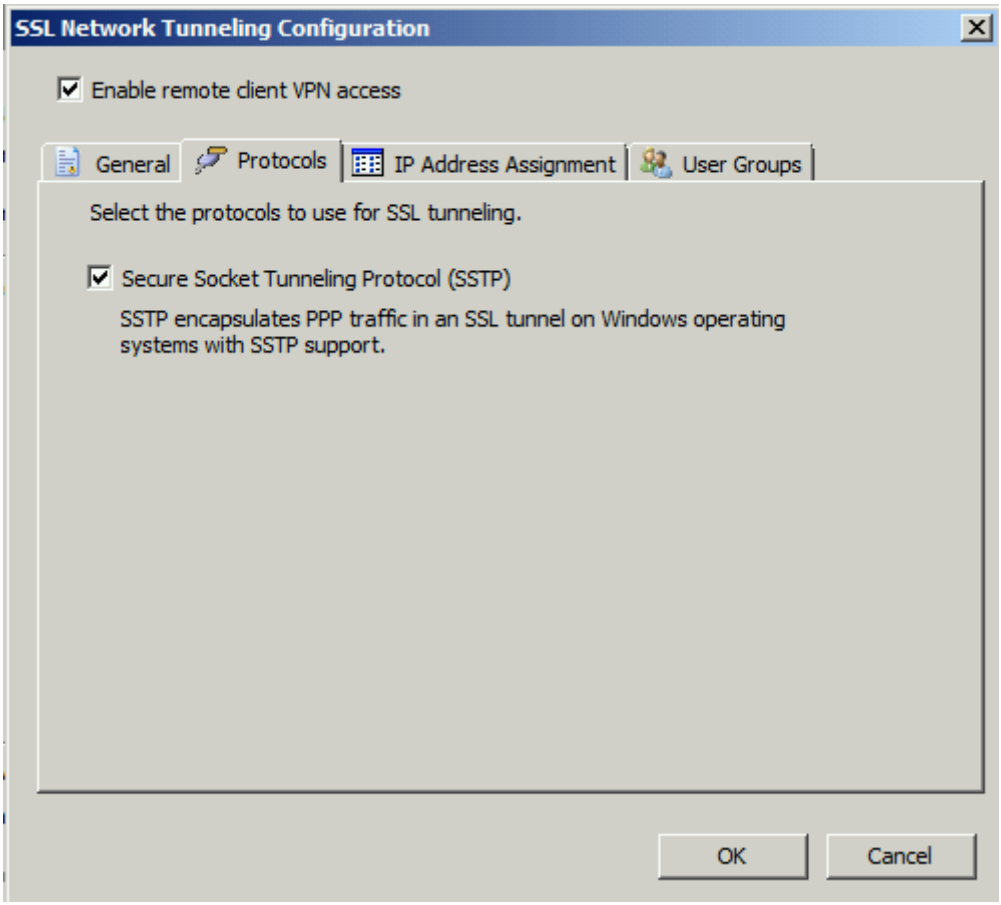

Figure 2: SSTP is enabled

On the IP address assignment tab specify how VPN clients should get IP addresses. It is possible to assign addresses from a static IP address pool or from a internal DHCP Server. If you use a static IP address pool, the IP address pool must be different from the IP address ranges assigned to the internal network object on the underlying Forefront TMG Server.

Attention:

In the case of static IP address ranges it is possible to exclude the IP range from the definition of your internal network.

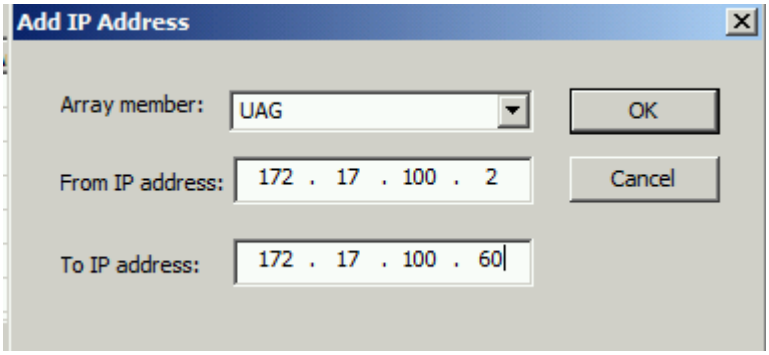

Figure 3: IP address range for SSTP clients

If you click the *Advanced* button it is possible to manually enter the IP address of DNS and WINS Servers used by the SSTP clients.

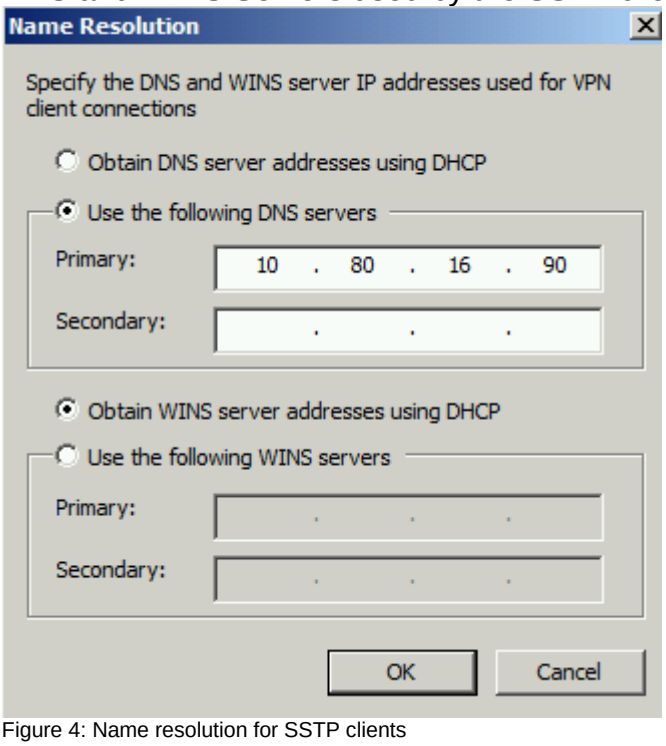

Figure 4: Name resolution for SSTP clients

On the *User groups* tab it is possible to limit SSTP VPN client access to specific user and usergroups and to specific IP addresses or IP address ranges which clients should be able to access.

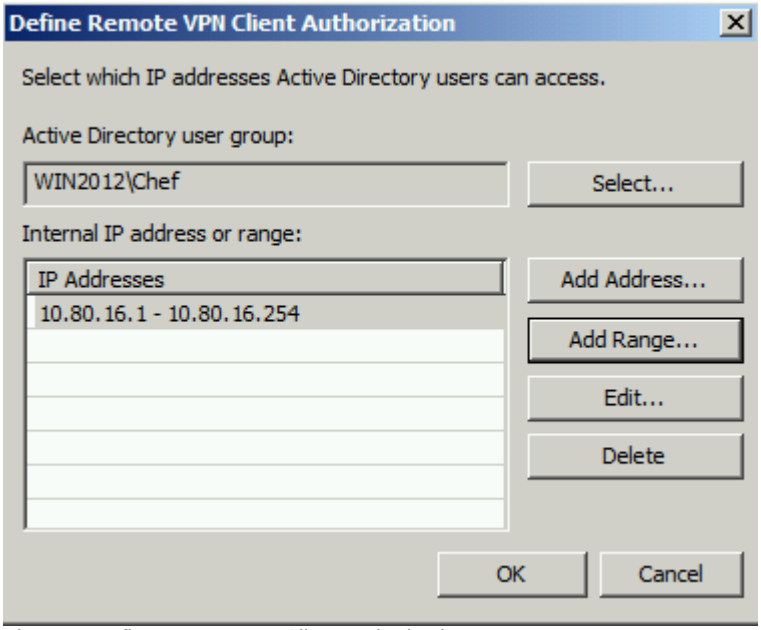

Figure 5: Define remote VPN Client Authorization

The next step is to publish the SSTP VPN connection to the portal used by SSTP. Right click the Portal trunk and click *Add Application* and enter the radio button *Client/server and legacy* and select remote Network Access.

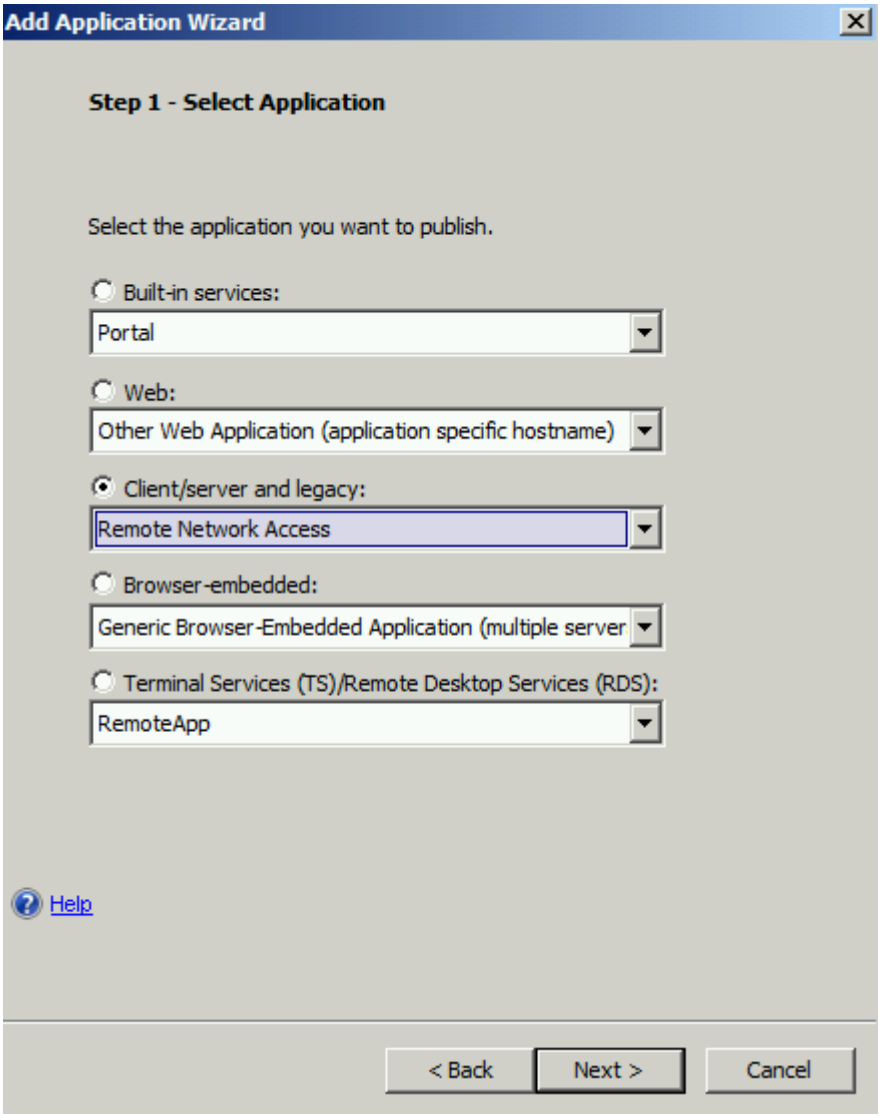

Figure 6: Publish SSTP to the portal

Enter an application name, an Endpoint access policy and if necessary in Step 4 another port used by Forefront UAG and if the application should be automatically started at user logon to the portal.

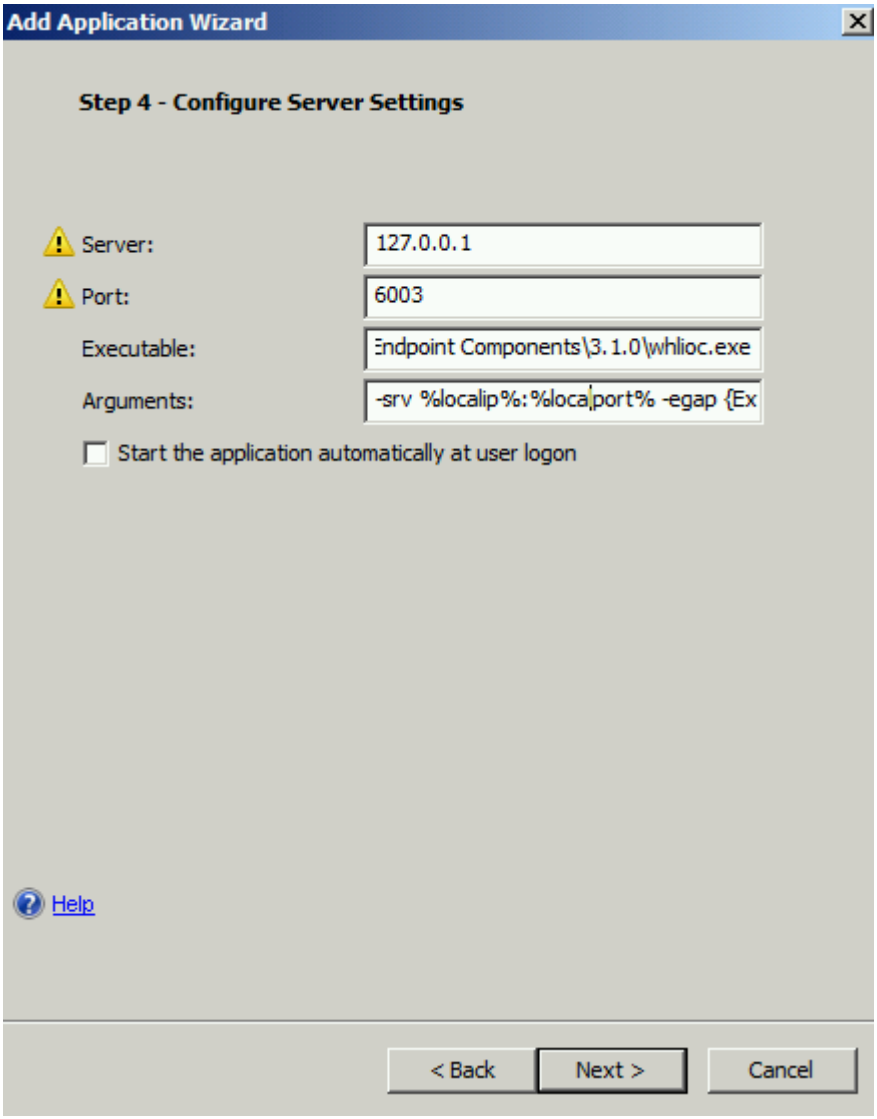

Figure 7: Configure Server settings

In Step 6 of the wizard it is possible to limit access to the SSTP application in the portal to specific users and user groups.

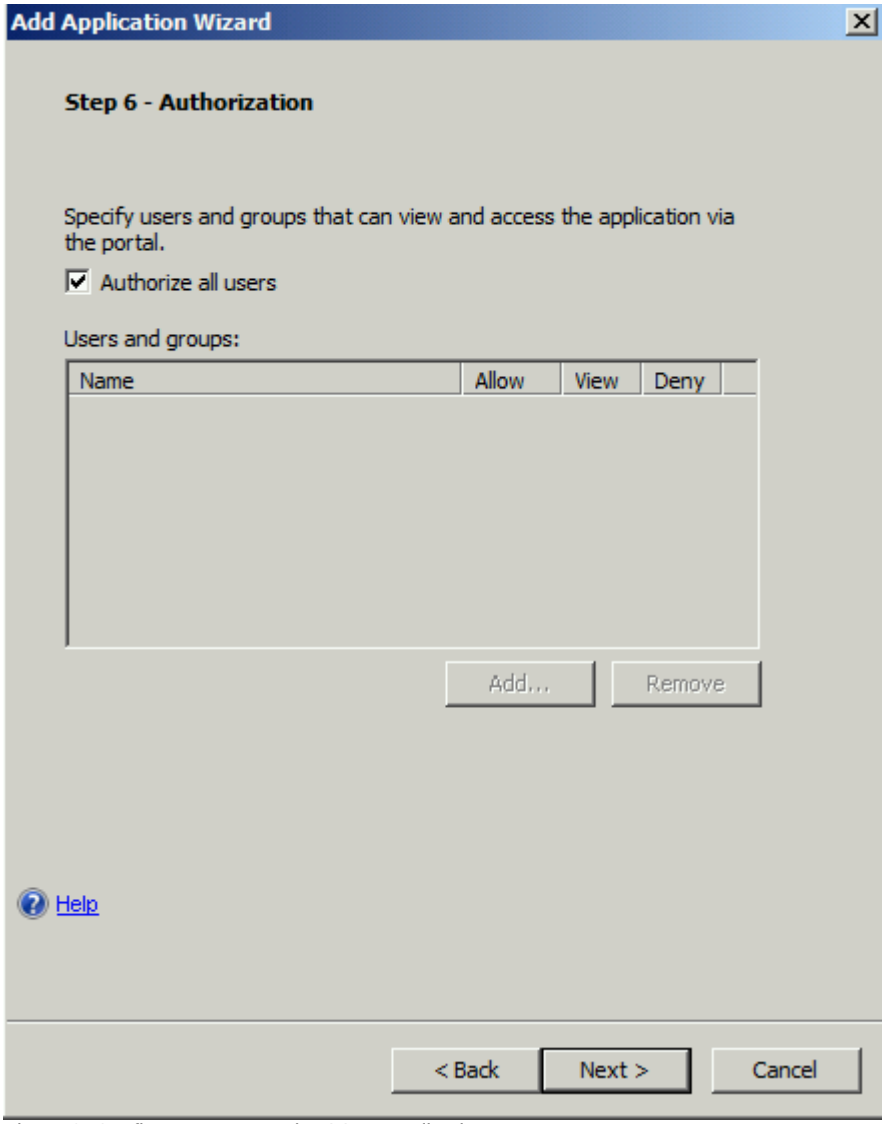

Figure 8: Configure access to the SSTP application

If the wizard has been finished, save and activate the configuration.
During the activation process, Forefront UAG/TMG configures the Windows Server Routing and Remote Access component.

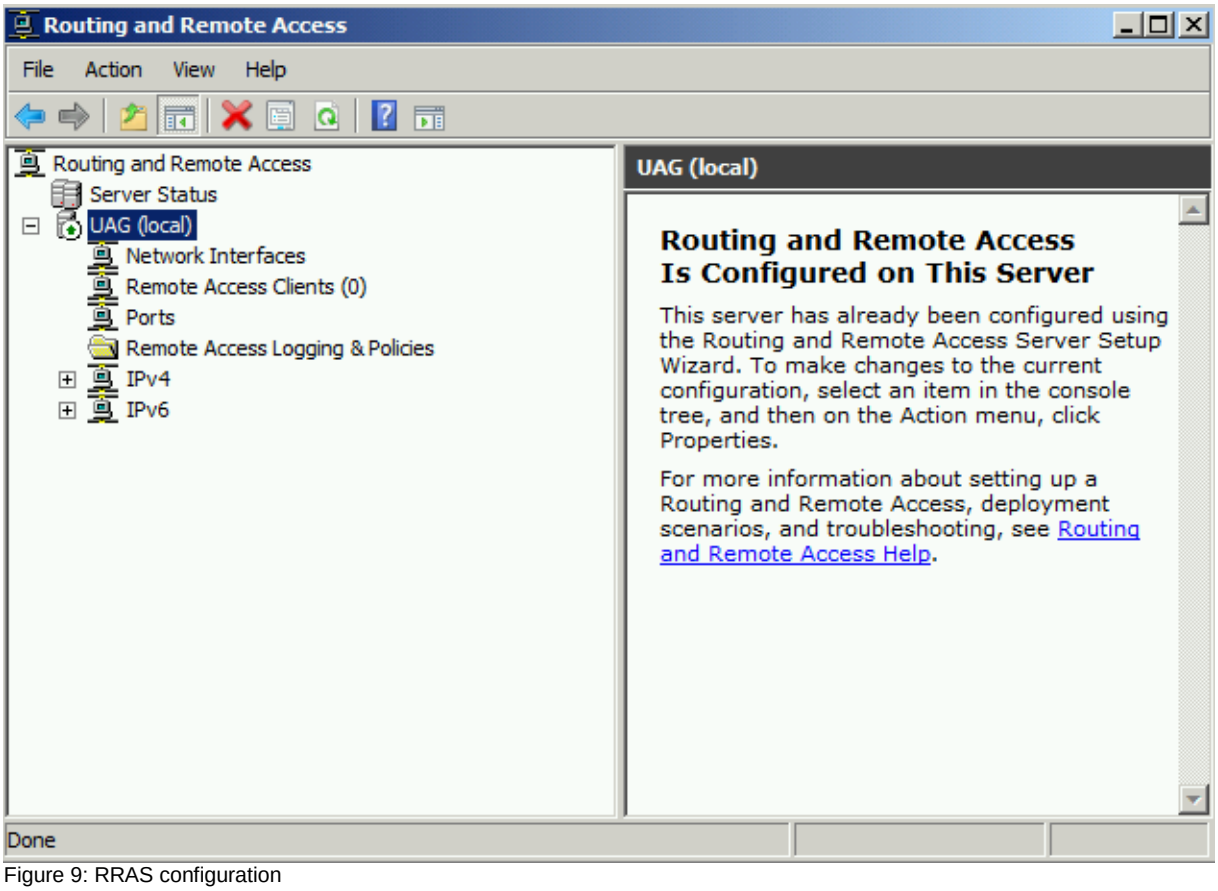

Figure 9: RRAS configuration

The UAG activation process also enable SSTP access in the Forefront TMG console.

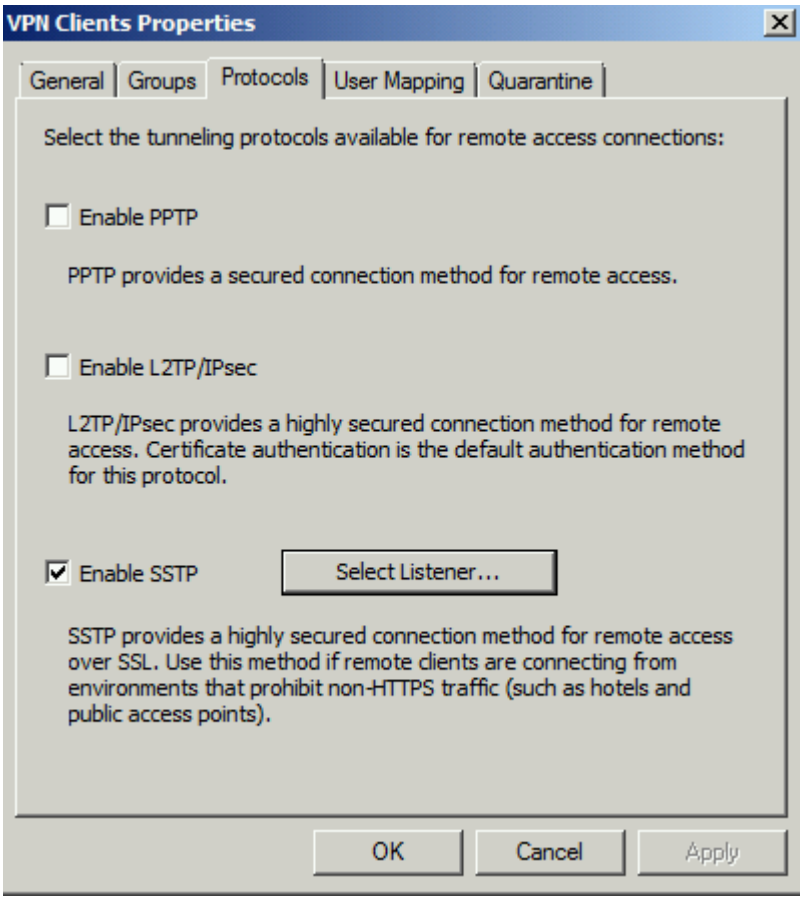

Figure 10: SSTP in Forefront TMG

Don’t be confused that there is no Weblistener configured for SSTP access in the Forefront TMG Management console. Forefront UAG will do the work.

Now it is time to test a SSTP connection from a Windows client. Log on to the Forefront UAG portal and launch the SSTP application.

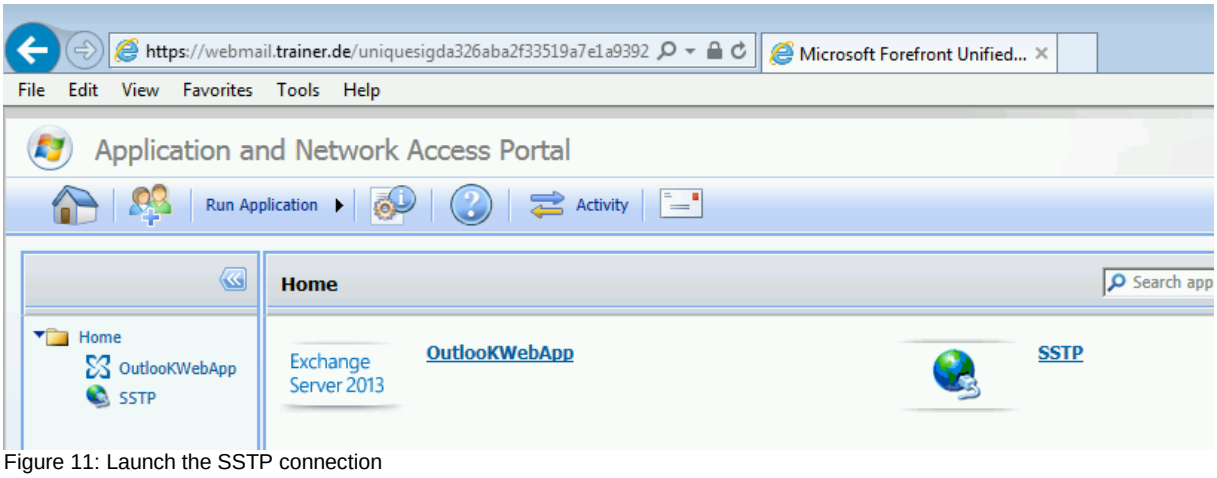

Figure 11: Launch the SSTP connection

If you are using a certificate from your own Certificate Authority make sure, that the Certificate Distribution Point (CDP) is access able from the Internet, else, the SSTP VPN connection cannot be established, because SSTP requires a CRL check.

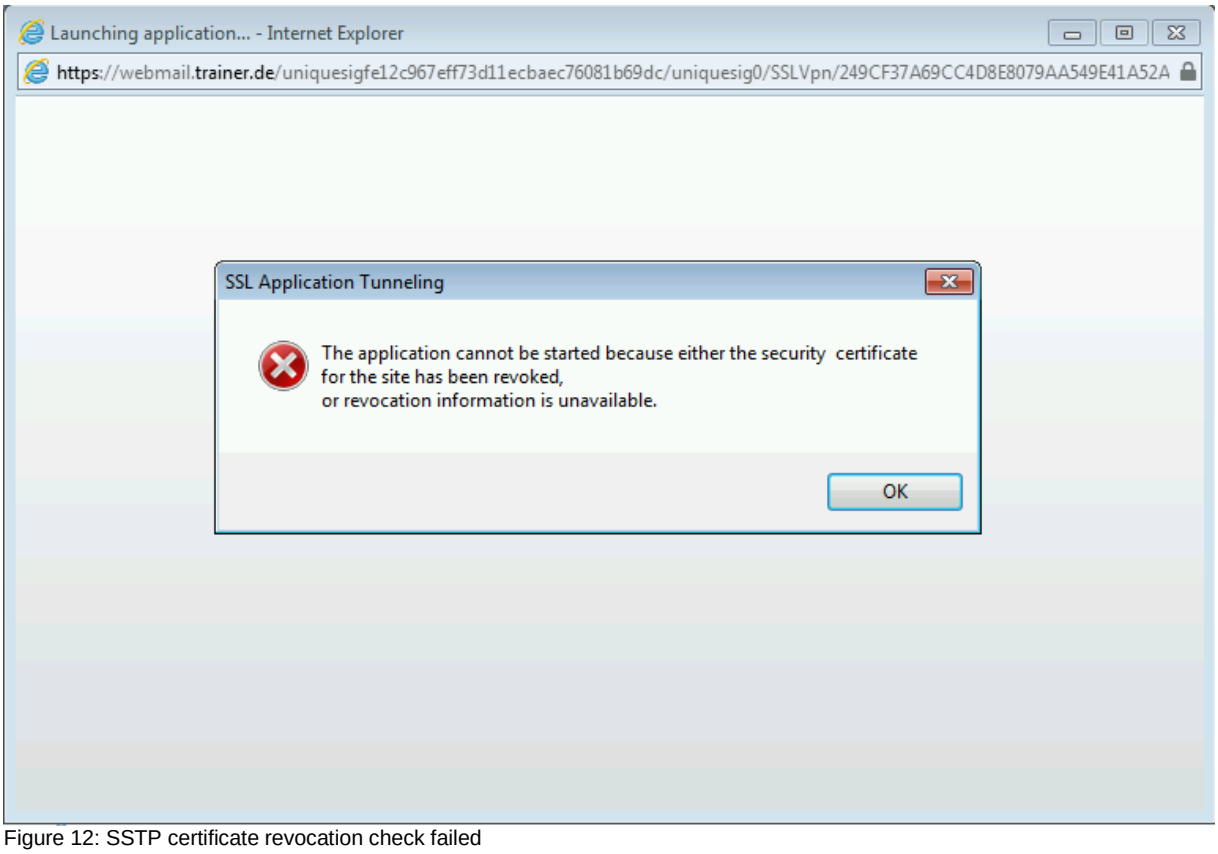

Figure 12: SSTP certificate revocation check failed

For testing purposes only it is possible to disable the Certificate revocation check on the client.

On the Windows client computer, open Regedit and create a DWORD value NoCertRevocationCheck under HKLM\System\CurrentControlSet\Services\SSTPSVC\Parameters. Set the value = 1.

The client is now connected with Forefront UAG Remote Network Access.

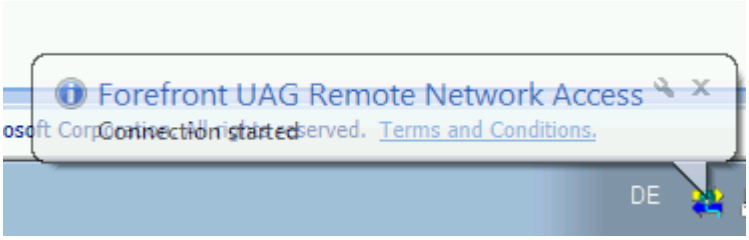

Figure 13: SSTP connection established

The SSTP connection installs a small application which allows users to get informed about the network connection status or to disconnect the SSTP connection.

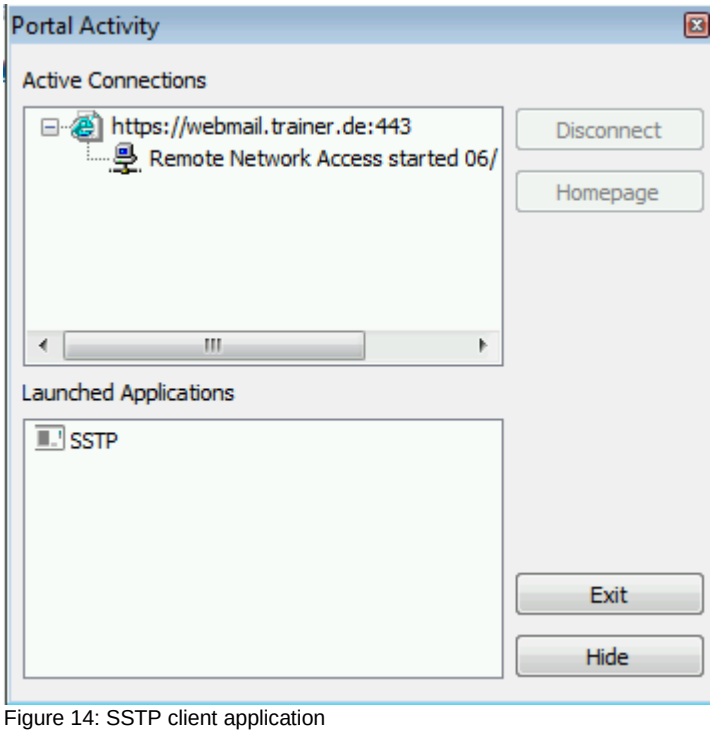

Figure 14: SSTP client application

The SSTP clients gets an IP address from the static IP address pool configured on the Forefront UAG Server.

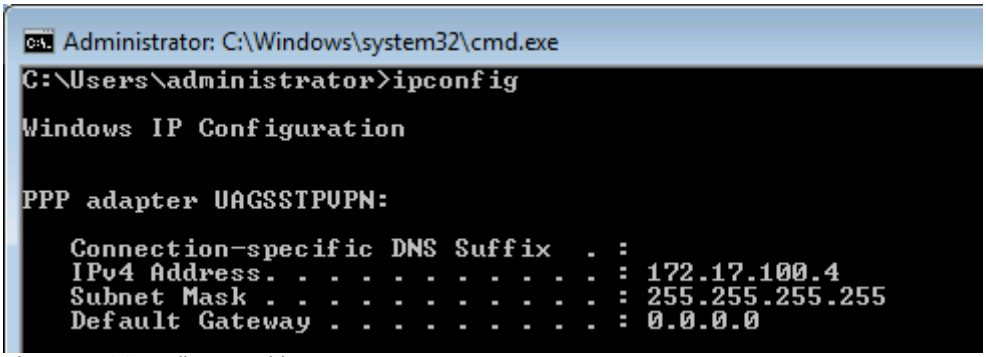

Figure 15: SSTP client IP address

The Forefront UAG Web Monitor allows you to monitor the SSTP connection

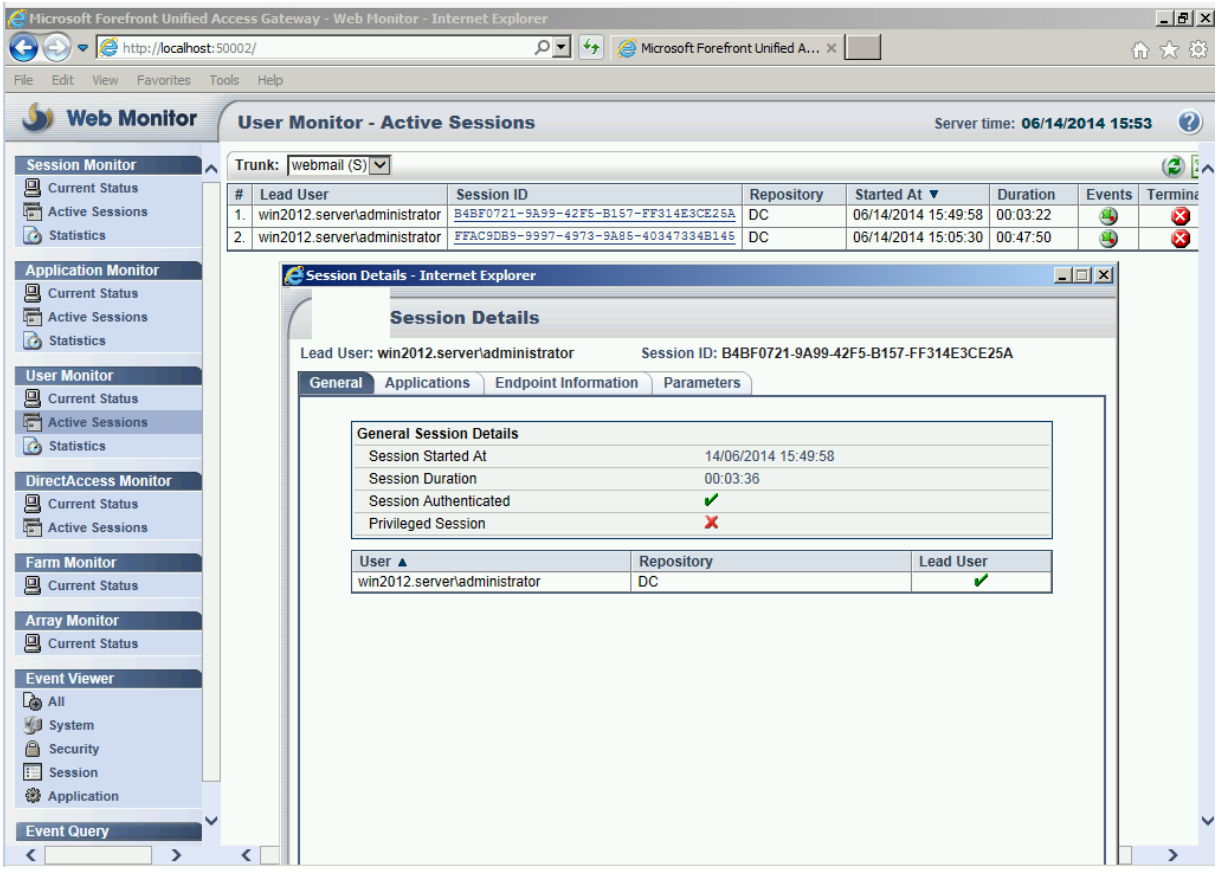

Figure 16: Forefront UAG Web Monitor

Conclusion

In this article I showed you how easy it is to publish a SSTP VPN connection with Forefront UAG for Windows Vista SP1 clients and higher.

Related links

Adding the SSTP Magic to the UAG Charm
http://blogs.technet.com/b/edgeaccessblog/archive/2009/07/05/adding-the-sstp-magic-to-the-uag-charm.aspx
How to publish a VPN SSTP using your UAG in a HTTPS trunk
http://blogs.technet.com/b/tugait/archive/2011/10/12/how-to-publish-a-vpn-sstp-using-your-uag-in-a-https-trunk.aspx
Microsoft Forefront UAG – Overview of Microsoft Forefront UAG
http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html
Forefront UAG technical overview
http://technet.microsoft.com/en-us/library/ee690443.aspx
Disable SSTP certificate verification check
http://support.microsoft.com/kb/947054/en-us